

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-242438

(43)Date of publication of application : 17.09.1996

(51)Int.Cl.

H04N 7/167

G11B 20/10

H04L 9/18

(21)Application number : 07-308004

(71)Applicant : LG ELECTRON INC

(22)Date of filing : 27.11.1995

(72)Inventor : PARK TAE JOON

(30)Priority

Priority number : 94 9431364 Priority date : 26.11.1994 Priority country : KR

(54) METHOD AND DEVICE FOR ILLEGAL VIEWING/COPYING PREVENTION OF DIGITAL VIDEO SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal viewing and copying by transmitting a scrambled bit stream and the encrypted key used for the scrambling through mutually different paths and descrambling the bit stream after decrypting the encrypted key with a smart card.

SOLUTION: A demodulation and error correction part 1 performs demodulation and RS decoding for an analog broadcast signal. An ATV decoder 2 descrambles the output of the correction part 1 according to descrambling information. A copying preventive process part 4 on the other hand separates a scrambled recording signal into a bit stream and a key stream and encrypts the key stream. Then the smart card 3 decrypts the encrypted key stream separated by the process part 4 and the index code of the ATV decoder 2 and outputs descrambled information KS to the decoder 2. Therefore authentication and key exchange are performed automatically to prevent illegal viewing and copying.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]

[Claim 1] A distinction stage which distinguishes whether scramble (scramble) of the data inputted was carried out distinguished from data by which scramble was carried out in said distinction stage after dividing into a bit stream and a key stream said data by which scramble was carried out Decode a separated key stream decipher key information and descrambling (descramble) of said separated bit stream is carried out according to key information If distinguished from a regeneration stage displayed in a display device and data by which scramble was carried out in said distinction stage According to record or copying mode record on a recording medium by data status with which a bit stream and a key stream were mixed and by which scramble was carried out A recording level which is mixed with a bit stream and recorded on a recording medium after dividing into a bit stream and a key stream data by which scramble was carried out and enciphering a separated key stream If distinguished from data by which scramble was carried out in said distinction stage after dividing into a bit stream and a key stream data by which scramble was carried out Decrypt a key stream separated according to "PPC" mode or "backup copy (Back-up Copy)" mode to key information by the side of record and illegal viewing and listening and a copy prevention method of a digital video system consisting of a transmission stage of decrypting a separated key stream twice and transmitting it to own key information and key information by the side of record and being able to perform simultaneous or selectively said regeneration stage a recording level and a transmission stage.

[Claim 2] Illegal viewing and listening and a copy prevention method of the digital video system according to claim 1 if distinguished from data by which scramble is not carried out in said distinction stage wherein data by which scramble is not carried out will not apply illegal viewing and listening and a copy preventing function.

[Claim 3] Illegal viewing and listening and a copy prevention method of the digital video system according to claim 1 wherein said regeneration stage decrypts a separated key stream with a decryption algorithm to an MPEG bit stream and deciphers key information.

[Claim 4] The 1st step where copying operation of said recording level enciphers a key stream to own key information The 2nd step that distinguishes whether a key stream enciphered in the 1st step is in "PPC" mode or it is in "backup copy" mode If distinguished from "PPC" mode in said 2nd step after enciphering to key information by the side of record of a key stream decrypted and transmitted to key information by the side of record The 3rd step that is inserted in a position corresponding to an index code and is recorded like a bit stream If distinguished from "backup copy" mode in said 2nd step it will encipher to key information by the side of record of a key stream decrypted and transmitted to own key information and key information by the side of record Illegal viewing and listening and a copy prevention method of the digital video system according to claim 1 inserting in a position corresponding to an index

code and consisting of the 4th step recorded like a bit stream after decrypting to key information on the self.

[Claim 5] The 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after said 3rd-step "PPC" mode operation separates a bit stream and a key stream. The 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record after enciphering to own key information. After enciphering a key stream transmitted in said 2nd transmission stage to key information by the side of record corresponding to an index code. Illegal viewing and listening and a copy prevention method of the digital video system according to claim 4 consisting of a recording level which is mixed to a bit stream transmitted in said 1st transmission stage and is recorded on a recording medium.

[Claim 6] If it reproduces by completing record by said recording level after dividing a reproduced bit stream ($S_{KS}(BS) + E^G(KS)$) into a bit stream ($S_{KS}(BS)$) and a key stream ($E^G(KS)$). A separation stage which inserts the index code IDX in a portion from which a key stream ($E^G(KS)$) was separated. An encryption stage which enciphers a key stream ($E^G(KS)$) separated in said separation stage to own key information. A decipherment stage which decipheres key information by decrypting a key stream enciphered in said encryption stage to own key information and an MPEG bit stream. Illegal viewing and listening and a copy prevention method of the digital video system according to claim 5 including a decryption stage which descrambles said separated bit stream ($S_{KS}(BS)$) based on key information deciphered in said decipherment stage.

[Claim 7] Said 4th-step "backup copy" mode operation. The 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after separating a bit stream and a key stream. The 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record of an enciphered key stream and own key information after enciphering to own key information. A key stream transmitted in said 2nd transmission stage is corresponded to an index code. Illegal viewing and listening and a copy prevention method of the digital video system according to claim 4 mixing to a bit stream transmitted in said 1st transmission stage and consisting of a recording level recorded on a recording medium after enciphering to key information by the side of record.

[Claim 8] If it reproduces by completing record by said recording level a reproduced bit stream ($S_{KS}(BS) + D_{AK}^{SC}[E^G(KS)]$). After separating a bit stream ($S_{KS}(BS)$) and a key stream ($D_{AK}^{SC}[E^G(KS)]$). A separation stage which inserts the index code IDX in a portion from which a key stream ($D_{AK}^{SC}[E^G(KS)]$) was separated. In an encryption stage which enciphers a key stream ($D_{AK}^{SC}[E^G(KS)]$) separated in said separation stage to own key information and said encryption stage. By decrypting a key stream enciphered twice to own key information and an MPEG bit stream. Illegal viewing and

listening and a copy prevention method of the digital video system according to claim 7 including a decipherment stage which deciphers key information and a decryption stage which descrambles a separated bit stream (S_{KS} (BS)) based on key information deciphered in said decipherment stage.

[Claim 9] If data by which scramble was carried out is inputted after dividing into a bit stream and a key stream said data by which scramble was carried out Decode a separated key stream decipher key information and said separated bit stream is descrambled based on deciphered key information By a regeneration stage displayed in a display device and data status with which a bit stream and a key stream were mixed when data by which scramble was carried out was inputted and by which scramble was carried out. Illegal viewing and listening and a copy prevention method of a digital video system consisting of a recording level recorded on a recording medium and being able to perform said regeneration stage and a recording level simultaneous or selectively.

[Claim 10] It is the key information which said regeneration stage decoded a separated key stream with a decryption algorithm to an MPEG bit stream deciphered key information and was deciphered Illegal viewing and listening and a copy prevention method of the digital video system according to claim 9 distinguishing a descrambling method.

[Claim 11] If it reproduces by completing record by said recording level after dividing a reproduced bit stream (S_{KS} (BS)+ E^G (KS)) into a bit stream (S_{KS} (BS)) and a key stream (E^G (KS)) A separation stage which inserts the index code IDX in a portion from which a key stream (E^G (KS)) was separated Own key information is received in a key stream (E^G (KS)) separated in said separation stage By decrypting a key stream enciphered twice to own key information and an MPEG bit stream in an encryption stage enciphered by an encryption algorithm and said encryption stage Based on key information deciphered in a decipherment stage which deciphers key information and said decipherment stage said separated bit stream (S_{KS} (BS)) is descrambled Illegal viewing and listening and a copy prevention method of the digital video system according to claim 9 including a decryption stage displayed in a display device.

[Claim 12] If a key stream enciphered to own key information at the time of a copy is transmitted A distinction stage which distinguishes whether it is in "backup copy" mode or it is in "PPC" mode The 1st transmission stage of decrypting and transmitting said key stream to key information by the side of record if distinguished from the [PPC] mode in said distinction stage After enciphering to key information by the side of record of a key stream transmitted in said 1st transmission stage an enciphered key stream is inserted in a position corresponding to an index code if distinguished from "backup copy" mode in the 1st recording level recorded on a recording medium like a bit stream and said distinction stage The 2nd transmission stage of decrypting a key stream twice and transmitting it to own key information and key information by the side of record After enciphering a key stream transmitted in said 2nd transmission

stage to key information by the side of record Illegal viewing and listening and a copy prevention method of a digital video system which are characterized by the 2nd recording level that inserts an enciphered key stream in a position corresponding to an index code and is recorded on a recording medium like a bit stream and a thing** and others.

[Claim 13] Illegal viewing and listening and a copy prevention method of the digital video system according to claim 12 transmitting it after said 1st transmission stage decrypts a key stream enciphered to the own key information A_k to the own key information A_k and decrypts it to key information aluminum by the side of record further.

[Claim 14] Said 2nd transmission stage a key stream enciphered to the own key information A_k Illegal viewing and listening and a copy prevention method of the digital video system according to claim 12 transmitting after decrypting twice to the own key information A_k and decrypting to key information aluminum by the side of record further.

[Claim 15] If a key stream ($E^G(KS)$) is detected at the time of reproduction of a recording medium it will distinguish from the "PPC" recording medium After enciphering a key stream to own key information decode for own key information and key information is deciphered A "PPC" mode reproduction stage which descrambles a bit stream using key information and an index code which were deciphered If a key stream ($D^{SC}_{AK}[E^G(KS)]$) decrypted to own key information at the time of reproduction of a recording medium is detected After distinguishing from a "backup copy" recording medium and enciphering twice to key information by the side of self and record Illegal viewing and listening and a copy prevention method of a digital video system decoding for own key information deciphering key information and consisting of deciphered key information and a "backup copy" mode reproduction stage which descrambles a bit stream using an index code.

[Claim 16] A recovery and an error correction means which carry out the strange recovery of the analog broadcasting signal and carry out RS decoding After dividing into a bit stream and a key stream a record signal which transmits said recovery and an output of an error correction means to record/playback equipment and is reproduced with its record/playback equipment and by which scramble was carried out A copy preventing process means to encipher a separated key stream and a decoder means to descramble a bit stream outputted from said recovery and an error correction means or a copy preventing process means based on descrambling information Illegal viewing and listening and a copy arrester of a digital video system having decoded a key stream enciphered by said copy preventing process means and constituting from a smart means to output to said decoder means as descrambling information.

[Claim 17] A decoder means by which said recovery and an error correction means were connected is connected to a smart means By decoding a key stream of said

decoder means for own key information with said smart card and outputting descrambling information to said decoder means. Illegal viewing and listening and a copy arrester of the digital video system according to claim 16 constituting so that an illegal viewing-and-listening preventing function may be performed.

[Claim 18] Illegal viewing and listening and a copy arrester of the digital video system according to claim 16 recording only after connecting to digital recording/playback equipment a copy preventing process means by which said recovery and an error correction means were connected.

[Claim 19] While connecting with a smart card a key stream line of a copy prevention means where said digital recording/playback equipment were connected. Connect a bit stream line to a decoder means and said copy preventing process means and a decoder means are connected. When said smart card decodes a key stream of said copy preventing process means corresponding to an index code of said decoder means for own key information and outputs to said decoder means. Illegal viewing and listening and a copy arrester of the digital video system according to claim 16 preventing illegal reproduction.

[Claim 20] Said copy preventing process means enciphers a key stream separated from regenerative data of digital recording/playback equipment at the time of recording-medium reproduction in "PPC" mode for own key information. Illegal viewing and listening and a copy arrester of the digital video system according to claim 19 transmitting to a smart card.

[Claim 21] Said copy preventing process means enciphers twice a key stream separated from regenerative data of digital recording/playback equipment at the time of reproduction medium reproduction in "backup copy" mode for own key information and it transmits to a smart card. Illegal viewing and listening and a copy arrester of the digital video system according to claim 19 by which it is characterized.

[Claim 22] RAM which memorizes key information that said copy preventing process means is peculiar to a smart card. An algorithm storage memory which stores an encryption algorithm. Claim 16 consisting of a processor which executes an enciphered program of said algorithm storage memory for key information on said RAM 18 or a digital video system indicated to either of Claim 19 and a copy arrester.

[Claim 23] The 1st algorithm storage memory in which said smart card stores a decryption algorithm program for bit SUTORIMU. The 2nd algorithm storage memory which stores an own decryption algorithm program. Illegal viewing and listening and a copy arrester of a digital video system given in either Claim 16 constituting from a ROM which stores own key information and RAM which carries out temporary storage of the key information on other smart cards 17 or Claim 19.

[Claim 24] A 1st copy preventing process means to encipher a separated key stream after dividing regenerative data of the 1st digital recording / playback equipment into a bit stream and a key stream. The 1st and 2nd smart card that decrypts a key stream enciphered by said 1st copy preventing process means to own key information and

key information by the side of recordAfter enciphering a key stream of said 1st smart card transmitted via said 2nd smart card for own key informationwith a bit stream from which an enciphered key stream was separated. A 2nd copy preventing process means to output to the 2nd digital recording / playback equipmentand to record on a recording mediumillegal viewing and listening of a digital video system ** constitutingand a copy arrester.

[Claim 25]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24 transmitting it to the 1st smart card after said 1st copy preventing process means enciphers a key stream to the own key information Ak.

[Claim 26]When said 1st smart card is in "PPC" modeafter decrypting a key stream of the 1st copy preventing process means to own key information and key information by the side of recordIllegal viewing and listening and a copy arrester of the digital video system according to claim 24 transmitting to the 2nd smart card.

[Claim 27]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24 mixing it with a bit stream of the 1st copy preventing process means after said 2nd copy preventing process means enciphers a key stream transmitted with the 2nd smart card to own key information aluminum.

[Claim 28]When said 1st smart card is in "backup copy" modelIllegal viewing and listening and a copy arrester of the digital video system according to claim 24 which are characterized by decoding to key information by the side of record after decoding a key stream of the 1st copy preventing process means twice to own key information.

[Claim 29]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24wherein said 2nd copy preventing process means enciphers a key stream transmitted from the 2nd smart card to own key information and mixes the enciphered key stream with a bit stream.

[Claim 30]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24 characterized by comprising the following.

RAM which stores key information that said 1st and 2nd copy preventing process means is peculiar to a smart card.

A processor which executes an enciphered program of said algorithm storage memory using an algorithm storage memory which stores an encryption algorithmand key information on said RAM.

[Claim 31]The 1st algorithm storage memory in which said 1st and 2nd smart card stores a decryption algorithm program for a bit streamIllegal viewing and listening and a copy arrester of the digital video system according to claim 24 constituting from a 2nd algorithm storage memory which stores an own decryption algorithm programa ROM which stores own key informationand RAM which carries out temporary storage of other smart key information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to illegal viewing and listening of a digital video system and copy prevention art. By decoding the key stream separated by introducing especially a smart card and setting up a descrambling method it is related with illegal viewing and listening / copy prevention method and the device of a digital video system which prevent illegal viewing and listening and a copy of an unapproved user.

[0002]

[Description of the Prior Art] Concern is concentrating on the embodiment of a Conditional Access (henceforth CA) system by the common digital video system for the prevention from illegal viewing and listening.

[0003] It is formal by broadcasting such a CA system with the gestalt by which scramble was carried out in the broadcasting signal by charged channel such as a cable TV and satellite broadcasting and only the user who paid money enables it to view and listen to a broadcast program to ** via descrambling. For example the satellite broadcasting receiver or the GrandAllinace (henceforth GA) system of a U.S. ATV standard has a function for supporting CA.

Scrambling / descrambling device used for satellite broadcasting like the video code (Video Cipher) of GI were also already daily-used.

[0004] The scrambling system for a common CA system is a video code (Video Cipher) system of GI.

If this carries out the scramble of the television signal transmitted to a regular member's descrambler by a charged TV system and broadcasts it on the basis of the U.S. Pat. No. 4613901 patent of Gilhouse. It is the system and method of descrambling selectively by a regular member's descrambler.

[0005] And what introduced and embodied the smart card to the video code (Video Cipher) system which performs descrambling is U.S. Pat. No. 5111504. This is the system of Gilhouse like "the information processor (Information Processor)" applicable to a descrambler and "a smart code (smart card)." It divides into "the protection element (Security Element)" for which it can substitute two and embodies in it.

[0006] Therefore if a scrambling system is embodied like drawing 1 with the application of said method a descrambling system will be embodied like drawing 2.

[0007] Namely the illegal viewing and listening arrester of the conventional digital video system. The scramble of the television signal Vi is carried out according to general standard information (Common Category Key) CK and initialization vector (Initialization Vector) PK. The television signal SVo by which scramble was carried

outand the scrambler 101 which outputs scrambling information ($E_{U(D)} E_{U(S)} (CK) E_{CK} (PK)$)The smart card 103 which enciphers the information ($A (D) A (S)$) for descrambling to descrambling information ($U (S)$) (Encryption)The information ($E_{A(D)} [E_{A(S)} (WK)]$) for descrambling of this smart card 103 is decoded (Decryption). It comprises the information processor 102 restored to the original television signal DVo by descrambling the transmission television signal SVo of said scrambler 101. A (D) is an attestation key (Authentication Key) of the information processor 102 hereA (S) is an attestation key of the smart card 103U (D) is the unit key (Unit Key) of said information processor 102and U (S) is an unit key of said smart card 103.

[0008]Under the present circumstancesthe 1st encryption machine 111 with which said scrambler 101 enciphers general key CK to the information ($U (D) U (S)$) for descramblingThe 2nd encryption machine 112 which enciphers initialization vector PK to general key CKIt comprises the 3rd encryption machine 113 which enciphers initialization vector PK to output $E_{CK} (PK)$ of said 2nd encryption machine 112and the scrambling execution end 114 which carries out the scramble of the television signal Vi according to the output WK of said 3rd encryption machine 113.

[0009]Hereafterthe process of a device of operation is explained conventionally which was constituted in this way.

[0010]When it is going to transmit a television signal by Transmission Systems Divisionthe scrambler 101 general standard information (Common Category Key) CK with the 1st encryption machine 111 Firstthe information ($U (D)$) for descramblingEncipher to ($U(S)$) and initialization vector information (Initialization Vector) PK is enciphered to general standard information CK by the 2nd encryption 112Initialization vector information PK is enciphered to the output ($E_{CK} (PK)$) of said 2nd encryption machine 112 with the 3rd encryption machine 113and it outputs to the scrambling processing end 114. Under the present circumstancesthe scrambling processing end 114 carries out the scramble of the television signal Vi on the basis of the output WK of the 3rd code machine 113. Herethe scrambling information WK appears in $E_{E_{CK}(PK)} (PK)$.

[0011]Encipherment information [as opposed to / by this / general standard information CK in the scrambler 101] ($E_{U(D)} E_{U(S)} (CK)$)The encipherment information ($E_{CK} (PK)$) over initialization vector information PK and the television signal SVo by which scramble was carried out will be transmitted to the information processor 102.

[0012]When the television signal SVo by which scramble was carried out is descrambled on the other handAfter the smart card 103 enciphers the information WK required for descrambling to the certification information ($A (D)$) of the information processor 102and own certification information ($A (S)$)The enciphered descrambling information ($E_{A (D)} [E_{A(S)} (WK)]$) is outputted to the information processor 102.

[0013]The information processor 102 decodes the enciphered information ($E_{A (D)} [E_{A(S)} (WK)]$) which was outputted from the smart card 103 by thisIt will restore to the original television signal DVo by descrambling the television signal SVo transmitted

from SUKUNRABURA 101 using this.

[0014]Here it is for improving security nature from illegal viewing and listening and a copy to apply encryption (Encryption) to the information transmission between the information processor 102 and the smart card 103.

[0015]For example the items (spec.) of a GA (Grand Alliance) high-definition TV system support a CA system and the function required for a transmission protocol is embodied. In the meaning of supporting all the usable descrambling methods and the key encryption (Key Encryption) methods the function embodied by this system is flexible (Flexible).

It is useful and the scramble of the bit stream can be carried out selectively and the flexibility (Flexibility) which can apply CA function per element stream is secured. Here scrambling means the process changed in order to mean making a data bit stream into irregularity (Random) and to protect information data from the conversion-to-its-own-use person who enciphers (Encryption) based on information data. That is a CA system makes irregular the data transmitted using a scrambler. While preventing from decoding to ** the decoder by the side of the conversion-to-its-own-use person who is going to view and listen to TV broadcast without notice. The decoder of the users to whom TV broadcast was permitted enables it to decode in normal the TV broadcast signal received by providing the information which formats a descrambler circuit.

[0016]Being able to embody the transmission protocol of MPEG for said operation in a format like drawing 3 such a transmission protocol has the two characteristics which support CA function.

[0017]It tells whether the scramble of the 1st 2-bit Transport-scrambling-control filled ** and the transmission stream was carried out and what kind of scrambling key when scramble was carried out was used.

[0018]The enciphered scrambling information is stored in such FIRUDO by the function which inserts each data into GA Transmission Systems Division using Transport-private-data FIRUDO in the adaptation (Adaptation) header of the 2nd transmission stream.

[0019]the transmission protocol of MPEG like drawing 3 which has said characteristic — a transmission header and a PES (Packetized Elementary Stream) header — and although an audio and a video data are transmitted respectively or simultaneously succeedingly. A transmission header comprises a ring header (Link Header) an adaptation header and a play load (payload) field.

[0020]Here link header (Link header) has a length of 4 bytes and length with a variable adaptation header.

[0021]Transport-scrambling-control FIRUDO is inserted in said link header. If the value of this FIRUDO is "00" they are Not-Scrambled and "10" they are the Even key and "11" and they are the Odd key and "01" it will be recognized to be Reserved.

[0022]And a flag bit and Transport-private-data FIRUDO are contained in an

adaptation header and a 1-bit Transport-private-data flag is included in said flag bit. The PES header of the transmission protocol of MPEG like drawing 3 is constituted like drawing 4.

[0023] Although FIRUDO for digital storage DSM like digital VCR exists in this PES header it is constituted including PES HEDDA FIRUDO which has a PES header flag field which has the length of 14 bits of such filled ** and variable length.

[0024] In said PES header flag field it constitutes including 1 bit CR (Copyright) flag 1 bit OC (original-or-copy) flag 2 bits PD flag 1 bit TM flag and 1-bit AC flag.

[0025] and PES header filled ** -- it has variable length and a partial area is set up by PD and TM which were contained to the PES header flag field and AC flag. Namely with a PES header flag a PTS/DTS field if the value of PD flag is "00" do not exist but if it is "10" 40 bits if it is "11" will become 80 bits and if the value of a DSM Trick Mode filled ** TM flag is "0" it does not exist it should be 8 bits when it will become 8 bits and an Additional Copy Info. filled ** AC flag will be set with "1" if it is "1."

[0026] Scrambling information was transmitted and by applying such a format showed the process descrambled using this information to drawing 5.

[0027] Herewith the key by which the descrambling system is used for the present descrambling the key as which the next was enciphered should be decoded and the descrambler must store 2 the "Odd key" and the "Even key." And the scrambling system must set and transmit the value of transport-scrambling-control FIRUDO in a link header with the method by which the present transmission stream is descrambled.

[0028] By this a descrambler will descramble and decode received data after distinguishing the "Even or Odd" key with the value of Transport-scrambling-control FIRUDO of the transmission header decoded with received data.

[0029] With namely the value of Transport-scrambling-control FIRUDO which the data of a format like drawing 5 was transmitted and was decoded with the smart card.

When the descrambler is descrambling the frame of eye K_{2n-1} watch by the Odd key A smart card decodes Transport-scrambling-control FIRUDO with the frame of eye K_{2n} watch descrambled next and such operation is performed one by one.

[0030] on the other hand the ATV decoder which performs CA function is embodied like drawing 6 although things can be carried out. Such an ATV decoder 110 will build the descrambler which needs high speed operation in the transmission demultiplexer 105 and a DES algorithm the stream SAIPA (Stream Cipher) algorithm using PN sequence etc. will perform descrambling. The key (Encrypted Key) enciphered by this ATV decoder 110 is decrypted with the smart card 103 (Decryption).

[0031] Here the interface of the smart card 103 and the ATV decoder 110 is made by ISO-7816 standards etc.

[0032] That is after the signal received with the tuner gets over by a recovery and the error correcting section 104 the error generated at the time of transmission is corrected via RS decoding and working example of drawing 6 is inputted into the transmission demultiplexer 105 of the ATV decoder 110 and is descrambled.

[0033] Under the present circumstances the microcontroller 109 calculates the control signal and data which were descrambled and transmits the encipherment information for descrambling to the smart card 103 and said smart card 103 decodes the transmitted encipherment information and it transmits it to the ATV decoder 110. Under the present circumstances the transmission JIMARUCHI plexor 105 will restore a compression video signal, a compression audio signal, a control signal and data based on descrambling information. Thereby after the video decoder's 107 elongating and making a note of a compression audio signal and carrying out temporary storage to 106 the storage data is outputted and an image is displayed and the audio decoder 108 elongates a compression audio signal and reproduces an audio. The microcontroller 109 deciphers the control signal and data which were outputted from the transmission JIMARUCHI plexor 105 and controls operation of said video decoder 107 and the audio decoder 108.

[0034] On the other hand a block SAIPA (Block-cipher) algorithm like DES and the stream SAIPA (Stream-cipher) algorithm using PN sequence are used generally most widely in the various methods used for encryption. However since even a cryptographic key performs encryption and decryption with a chisel key management (Key Management) and key distribution (Key Distribution) are difficult for such a method.

[0035] Therefore a public key (Public-Key) cipher system like U.S. Pat. No. 4200770 was proposed as a solution to this. This method enciphers using the public key which is an exhibited key and decodes by an own secret key (Secret key). And U.S. Pat. No. 4405829 has improved such a public key encryption-ized method embodied with the encryption system and it is known as an RSA encryption algorithm.

[0036]

[Problem(s) to be Solved by the Invention] However said public key encryption-ized method has the demerit of being unsuitable in high-speed encryption. Although the CA system aimed at preventing illegal viewing and listening to the program distributed via DSM like digital VCR there was no method of protecting against an illegal copy.

[0037] Namely although the protection to the program supplied by a recording medium like DSM means prevention of an illegal copy, being hard to apply the copy prevention (Copy Protection) method applied to the existing analog VCR system to the storage of a digital system the research to the copy preventing system for DSM is not independently progressing until now.

[0038] Therefore are for this invention solving this problem and the purpose The bit stream by which scramble was carried out and the enciphered key which were used for scrambling are transmitted in a mutually different course By descrambling a bit stream and preventing from performing normal decoding only at a bit stream based on the information after decoding the enciphered key with a smart card It is in providing illegal viewing and listening and the copy prevention method of the digital video system which prevents illegal viewing and listening and a copy.

[0039]Such this invention makes a PPV (Pay Per View) function much more powerful including the function which introduces a smart card with a CA system and checks a fee automatically (checking)By adding various functions by substitution of a smart cardupgrade (Upgrade) of the system performance can be carried out easily.

[0040]Since this invention can carry out sharp reduction of the key daily dose of the data protected since transmission data is separated and attestation and a key exchange process are automatically performed at the time of connection between digital VCR for the time of power-on or recordingIt does not operate and the reliability of a protection feature is made to improve further in an illegal smart card.

[0041]

[Means for Solving the Problem]Illegal viewing and listening and a copy prevention method of a digital video system by this inventionA distinction stage which distinguishes whether scramble (scramble) of the data inputted was carried outIf distinguished from data by which scramble was carried out in said distinction stageafter dividing into a bit stream and a key stream said data by which scramble was carried outDecode a separated key streamdecipher key informationand descrambling (descramble) of said separated bit stream is carried out according to key informationIf distinguished from a regeneration stage displayed in a display deviceand data by which scramble was carried out in said distinction stageRecord on a recording medium by data status with which a bit stream and a key stream were mixed according to record or copying mode and by which scramble was carried outA recording level which is mixed with a bit stream and recorded on a recording medium after dividing into a bit stream and a key stream data by which scramble was carried out and enciphering a separated key streamIf distinguished from data by which scramble was carried out in said distinction stageafter dividing into a bit stream and a key stream data by which scramble was carried outDecrypt a key stream separated according to "PPC" mode or "backup copy (Back-up Copy)" mode to key information by the side of recordand transmitIt consists of a transmission stage of decrypting a separated key stream twice and transmitting it to own key information and key information by the side of recordand said regeneration stagea recording leveland a transmission stage can be performed simultaneous or selectivelyand the above-mentioned purpose is attained by that.

[0042]According to a certain embodimentIf distinguished from data by which scramble is not carried out in said distinction stagedata by which scramble is not carried out will not apply illegal viewing and listening and a copy preventing function.

[0043]According to a certain embodimentsaid regeneration stage decrypts a separated key stream with a decryption algorithm to an MPEG bit streamand deciphers key information. In a certain embodimentcopying operation of said recording levelThe 1st step that enciphers a key stream to own key informationand the 2nd step that distinguishes whether a key stream enciphered in the 1st step is in "PPC" modeor it is in "backup copy" modeIf distinguished from "PPC" mode in said 2nd

step after enciphering to key information by the side of record of a key stream decrypted and transmitted to key information by the side of record. The 3rd step that is inserted in a position corresponding to an index code and is recorded like a bit stream. If distinguished from "backup copy" mode in said 2nd step, it will encipher to key information by the side of record of a key stream decrypted and transmitted to own key information and key information by the side of record. After decrypting to key information on the self, it inserts in a position corresponding to an index code and is that it is ***** with the 4th step recorded like a bit stream.

[0044] In a certain embodiment, said 3rd-step "PPC" mode operation. The 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after separating a bit stream and a key stream. The 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record after enciphering to own key information. A recording level which is mixed to a bit stream transmitted in said 1st transmission stage and is recorded on a recording medium after enciphering a key stream transmitted in said 2nd transmission stage to key information by the side of record corresponding to an index code. If it reproduces by completing record according to said recording level in a certain embodiment, which is that it is ***** After dividing a reproduced bit stream ($S_{KS}(BS) + E^G(KS)$) into a bit stream ($S_{KS}(BS)$) and a key stream ($E^G(KS)$). A separation stage which inserts the index code IDX in a portion from which a key stream ($E^G(KS)$) was separated and an encryption stage which enciphers a key stream ($E^G(KS)$) separated in said separation stage to own key information. A decipherment stage which decipheres key information by decrypting a key stream enciphered in said encryption stage to own key information and an MPEG bit stream. A decryption stage which descrambles said separated bit stream ($S_{KS}(BS)$) based on key information deciphered in said decipherment stage is included.

[0045] In a certain embodiment, said 4th-step "backup copy" mode operation. The 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after separating a bit stream and a key stream. The 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record of an enciphered key stream and own key information after enciphering to own key information. After enciphering a key stream transmitted in said 2nd transmission stage to key information by the side of record corresponding to an index code, it mixes to a bit stream transmitted in said 1st transmission stage and is that it is ***** with a recording level recorded on a recording medium.

[0046] If it reproduces by completing record according to said recording level in a certain embodiment, a reproduced bit stream ($S_{KS}(BS) + D_{AK}^{SC}[E^G(KS)]$). After separating a bit stream ($S_{KS}(BS)$) and a key stream ($D_{AK}^{SC}[E^G(KS)]$). A separation stage which inserts the index code IDX in a portion from which a key stream ($D_{AK}^{SC}[E^G(KS)]$) was separated. In an encryption stage which enciphers twice a key stream ($D_{AK}^{SC}[E^G(KS)]$).

separated in said separation stage to own key information and said encryption stage by decrypting a key stream enciphered twice to own key information and an MPEG bit stream. A decipherment stage which decipheres key information and a decryption stage which descrambles a separated bit stream ($S_{KS}(BS)$) based on key information deciphered in said decipherment stage are included.

[0047] Illegal viewing and listening and a copy prevention method of a digital video system by this invention. If data by which scramble was carried out is inputted after dividing into a bit stream and a key stream, said data by which scramble was carried out is decoded. A separated key stream decipher key information and said separated bit stream is descrambled based on deciphered key information. By a regeneration stage displayed in a display device and data status with which a bit stream and a key stream were mixed when data by which scramble was carried out was inputted and by which scramble was carried out. It consists of a recording level recorded on a recording medium, said regeneration stage and a recording level can be performed simultaneously or selectively and the above-mentioned purpose is attained by that.

[0048] According to a certain embodiment, said regeneration stage decodes a separated key stream with a decryption algorithm to an MPEG bit stream, decipheres key information, is the deciphered key information and distinguishes a descrambling method.

[0049] If it reproduces by completing record according to said recording level in a certain embodiment after dividing a reproduced bit stream ($S_{KS}(BS) + E^a(KS)$) into a bit stream ($S_{KS}(BS)$) and a key stream ($E^a(KS)$). A separation stage which inserts the index code IDX in a portion from which a key stream ($E^a(KS)$) was separated. Own key information is received in a key stream ($E^a(KS)$) separated in said separation stage. By decrypting a key stream enciphered twice to own key information and an MPEG bit stream in an encryption stage enciphered by an encryption algorithm and said encryption stage. A decipherment stage which decipheres key information and a decryption stage which descrambles said separated bit stream ($S_{KS}(BS)$) and is displayed in a display device based on key information deciphered in said decipherment stage are included.

[0050] Illegal viewing and listening and a copy prevention method of a digital video system by this invention. If a key stream enciphered to own key information at the time of a copy is transmitted, a distinction stage which distinguishes whether it is in "backup copy" mode or it is in "PPC" mode. The 1st transmission stage of decrypting and transmitting said key stream to key information by the side of record if distinguished from the "PPC" mode in said distinction stage. After enciphering to key information by the side of record of a key stream transmitted in said 1st transmission stage, an enciphered key stream is inserted in a position corresponding to an index code if distinguished from "backup copy" mode in the 1st recording level recorded on a recording medium like a bit stream and said distinction stage. The 2nd transmission stage of decrypting a key stream twice and transmitting it to own key information and key information by the side of record. After enciphering a key stream transmitted in

said 2nd transmission stage to key information by the side of record. An enciphered key stream is inserted in a position corresponding to an index code it is that it is ***** with the 2nd recording level recorded on a recording medium like a bit stream and the above-mentioned purpose is attained by that.

[0051] According to a certain embodiment, said 1st transmission stage is transmitted after decrypting a key stream enciphered to the own key information A_k to the own key information A_k and decrypting to key information aluminum by the side of record further.

[0052] According to a certain embodiment, said 2nd transmission stage is transmitted after decrypting twice a key stream enciphered to the own key information A_k to the own key information A_k and decrypting it to key information aluminum by the side of record further.

[0053] Illegal viewing and listening and a copy prevention method of a digital video system by this invention. If a key stream ($E^q(KS)$) is detected at the time of reproduction of a recording medium, it will distinguish from the "PPC" recording medium. After enciphering a key stream to own key information, decode for own key information and key information is deciphered. A "PPC" mode reproduction stage which descrambles a bit stream using key information and an index code which were deciphered. If a key stream ($D_{AK}^{sc}[E^q(KS)]$) decrypted to own key information at the time of reproduction of a recording medium is detected. After distinguishing from a "backup copy" recording medium and enciphering twice to key information by the side of self and record. It decodes for own key information. Key information is deciphered. It is that it is ***** with deciphered key information and a "backup copy" mode reproduction stage which descrambles a bit stream using an index code and the above-mentioned purpose is attained by that.

[0054] Illegal viewing and listening and a copy arrester of a digital video system by this invention. A recovery and an error correction means which carry out the strange recovery of the analog broadcasting signal and carry out RS decoding. After dividing into a bit stream and a key stream, a record signal which transmits said recovery and an output of an error correction means to record/playback equipment and is reproduced with its record/playback equipment and by which scramble was carried out. A copy preventing process means to encipher a separated key stream and a decoder means to descramble a bit stream outputted from said recovery and an error correction means or a copy preventing process means based on descrambling information. A key stream enciphered by said copy preventing process means is decoded. It constitutes [**] with a smart means to output to said decoder means as descrambling information and the above-mentioned purpose is attained by that.

[0055] In a certain embodiment, a decoder means by which said recovery and an error correction means were connected is connected to a smart means. By decoding a key stream of said decoder means for own key information with said smart card and outputting descrambling information to said decoder means, it constitutes so that an

illegal viewing-and-listening preventing function may be performed.

[0056]According to a certain embodiment a copy preventing process means by which said recovery and an error correction means were connected records only after being connected to digital recording/playback equipment.

[0057]While connecting to a smart card a key stream line of a copy prevention means where said digital recording/playback equipment were connected in a certain embodiment a bit stream line is connected to a decoder means. Illegal reproduction is prevented when said copy preventing process means and a decoder means are connected and said smart card decodes a key stream of said copy preventing process means corresponding to an index code of said decoder means for own key information and outputs to said decoder means.

[0058]According to a certain embodiment said copy preventing process means enciphers a key stream separated from regenerative data of digital recording/playback equipment at the time of recording-medium reproduction in "PPC" mode for own key information and transmits it to a smart card.

[0059]According to a certain embodiment said copy preventing process means enciphers twice for own key information and transmits a key stream separated from regenerative data of digital recording/playback equipment at the time of reproduction medium reproduction in "backup copy" mode to a smart card.

[0060]In a certain embodiment said copy preventing process means it is that it is ***** with RAM which memorizes key information peculiar to a smart card and an algorithm storage memory which stores an encryption algorithm and a processor which executes an enciphered program of said algorithm storage memory for key information on said RAM.

[0061]The 1st algorithm storage memory in which said smart card stores a decryption algorithm program for bit SUTORIMU in a certain embodiment it constitutes [**] with the 2nd algorithm storage memory which stores an own decryption algorithm program ROM which stores own key information and RAM which carries out temporary storage of the key information on other smart cards.

[0062]Illegal viewing and listening and a copy arrester of a digital video system by this invention A 1st copy preventing process means to encipher a separated key stream after dividing regenerative data of the 1st digital recording / playback equipment into a bit stream and a key stream The 1st and 2nd smart card that decrypts a key stream enciphered by said 1st copy preventing process means to own key information and key information by the side of record After enciphering a key stream of said 1st smart card transmitted via said 2nd smart card for own key information with a bit stream from which an enciphered key stream was separated. It outputs to the 2nd digital recording / playback equipment and constitutes [**] with a 2nd copy preventing process means to record on a recording medium and the above-mentioned purpose is attained by that.

[0063]According to a certain embodiment after said 1st copy preventing process

means enciphers a key stream to the own key information Akit is transmitted to the 1st smart card.

[0064]According to a certain embodimentwhen it is [said 1st smart card] in "PPC" modeafter decrypting a key stream of the 1st copy preventing process means to own key information and key information by the side of recordit is transmitted to the 2nd smart card.

[0065]According to a certain embodimentsaid 2nd copy preventing process means mixes with a bit stream of the 1st copy preventing process means a key stream transmitted with the 2nd smart cardafter enciphering to own key information aluminum.

[0066]According to a certain embodimentwhen it is in "backup copy" modesaid 1st smart card decodes it to key information by the side of recorderafter it decodes a key stream of the 1st copy preventing process means twice to own key information.

[0067]According to a certain embodimentsaid 2nd copy preventing process means enciphers a key stream transmitted from the 2nd smart card to own key informationand mixes the enciphered key stream with a bit stream.

[0068]In a certain embodimentsaid 1st and 2nd copy preventing process meansit constitutes [**] with RAM which stores key information peculiar to a smart cardan algorithm storage memory which stores an encryption algorithmand a processor which executes an enciphered program of said algorithm storage memory using key information on said RAM.

[0069]In a certain embodimentsaid 1st and 2nd smart cardThe 1st algorithm storage memory which stores a decryption algorithm program for a bit streamit constitutes [**] with the 2nd algorithm storage memory which stores an own decryption algorithm programROM which stores own key informationand RAM which carries out temporary storage of other smart key information.

[0070]

[Embodiment of the Invention]Hereafterthis invention is explained in detail with reference to an accompanying drawing.

[0071]This invention can be applied to all the record/playback equipment which can record and reproduce a digital signaland makes DVCR one working example in this invention for the facilities of explanation.

[0072]Thereforethe recovery and the error correcting section 1 which carry out the strange recovery of the broadcasting signal of an analogand carry out RS decoding as working example of this invention is shown in drawing 7The ATV decoder 2 which descrambles said recovery and the output of the error correcting section 1 based on descrambling informationThe copy preventing process part 4 which divides into a bit stream and a key stream the record signal by which scramble was carried outand enciphers the separated key streamit constitutes from the smart card 3 which decodes the index code of the key stream separated and enciphered in this copy preventing process part 4and said ATV decoder 2and outputs the descrambling

information KS to said ATV decoder 2.

[0073]RAM17 in which said copy preventing process part 4 stores key information peculiar to a smart card as shown in drawing 8It constitutes from the algorithm stores dept. 18 which stores an encryption algorithm and the processor 16 which executes the enciphered program of said algorithm stores dept. 18 for the key information on said RAM17.

[0074]The 1st algorithm stores dept. 12 in which said smart card 3 stores the decryption algorithm for a bit stream as shown in drawing 9The 2nd algorithm stores dept. 13 which stores an own decryption algorithmROM14 which stores own key information and RAM15 which carry out temporary storage of the key information on other smart cardsIt constitutes from the processor 11 which performs encryption or decryption to the key information stored in said ROM14 or RAM15 with the storage algorithm of said 1st and 2nd algorithm stores depts 12 and 13.

[0075]Under the present circumstanceswhen said processors 11 and 16 can be constituted from WAIYADO logic (Wired Logic)or can use a microprocessor and use a microprocessorthey will build in the encryption algorithm for a smart card by a program.

[0076]Hereafterthe operation and the operation effect of this invention which were constituted in this way are explained.

[0077]Although an MPEG bit stream is transmitted in drawing 11 (a) thru/or a format as shown in (c) by this inventionDrawing 11 (a) is a format by which scramble is not carried outdrawing 11 (b) is the format by which scramble was carried out to the bit stream and drawing 11 (c) is the format to which the scramble of the bit stream was carried out selectively.

[0078]In this inventionwhen scramble is carried out to an MPEG bit streamif protection (protection) is added with any gestaltena premise will be carried out.

[0079]Thereforewhen the stream data ($S_{KS}(BS)+E^a(KS)$) in which the scramble of drawing 11 (b) or the format as shown in (c) was carried out to the copy preventing process part 4 are inputtedIf it separates into drawing 11 (d) thru/or a bit stream ($S_{KS}(BS)+IDX$) as shown in (e) and a key stream ($E^a(KS)$) by splitter (Splitter) as shown in drawing 10 and a recording mode is performedIt is enciphered further and said separated key stream ($E^a(KS)$) is transmitted to the smart card 3.

[0080]Heresince illegal viewing and listening and a copy preventing function are applied only to the portion by which scramble was carried out when the scramble of the bit stream is carried out selectively as shown in drawing 11 (c) a partial protection feature can be performed.

[0081]Firstas shown in drawing 11 (a) when the bit stream by which scramble is not carried out is transmittedEven if the bit stream to which it strange-restored and which was decoded by the recovery and the error correcting section 1 is inputted into the copy preventing process part 4 data is not transmitted to the smart card 3A bit stream is decoded without the ATV decoder 2 into which the bit stream of said

recovery and the error correcting section 1 was inputted also transmitting data to said smart card 3. Therefore restriction [what] is also lost to viewing and listening and a copy.

[0082] The video and the audio signal which are outputted here from the signal inputted into a recovery and the error correcting section 1 from a tuner and the ATV decoder 2 are an analog signal. The signal outputted from a tuner is a signal by which VSB abnormal conditions were carried out from GA bit stream. And a bit stream and a key stream are the digital signals for digital DVCR among input output signals. Under the present circumstances if it records a bit stream will be recorded on digital VCR and this recorded bit stream will be reproduced with general digital VCR. That is since there is no data transmitted to the smart card 3 in order that there may be no key information even if it passes a splitter as the MPEG bit stream which does not require scrambling is inputted into the copy preventing process part 4 and it is shown in drawing 10 When scrambling does not start any restriction cannot be found in viewing and listening and a copy.

[0083] Separate into a bit stream and a key stream and this invention is transmitted with a line different respectively when performing recording or a copy preventing function but. The information about a copy prevention method is carried and transmitted to addition copy information (Additional Copy Info.) FIRUDO in a PES header.

[0084] Under the present circumstances since it is in the state where the information about a key was removed even if it transmits the bit stream without the enciphered key by which scramble was carried out by a public channel when it flows into a conversion-to-its-own-use person descrambling cannot be performed to **. And since it is enciphered further and the separated key is transmitted a bit stream cannot be descrambled when there is no decoding algorithm. Therefore although this invention uses arbitrary FIRUDO with an MPEG transmission protocol for starting illegal viewing and listening and the prevention from a copy for the bit stream by which scramble was carried out a copy preventing function is applied.

[0085] First by the decoder 2 if it changes "Transport-scrambling-control filled" into "Not Scrambled" mode since descrambling is not performed the conversion-to-his-own-use person cannot operate said FIRUDO. Since it determines it that whether copy prevention being made to be carried out by "Transport-scrambling-control filled" and a copy are possible (free-copy) for such a copy prevention method whether it is made to become Only by operating this FIRUDO the conversion-to-his-own-use person cannot cancel a copy preventing function.

[0086] By next the way a conversion-to-his-own-use person corrects "addition copy information (Additional Copy Info.) filled" in a PES header. Since correction of this FIRUDO transforms a protective method and the protective method itself is not disassembled big damage is not done to a copy preventing function.

[0087] The copy prevention method supported by this invention which has such a

feature PPV (Pay Per View) and the PPP (Pay Per Play) function which are CA functions are considered as the default (Default) and there are the "No Copy" method a "PPC (Pay Per Copy)" method and the "Back-up Copy" method.

[0088] On other videotapes the "No Copy" method is a copy the method of keeping from the ability to do at all here and the "PPC" method Receive a fee for every copy once and the "Back-up Copy" method It is a method which can display in normal the videotape copied when digital VCR by the side of other copied the videotape played with digital VCR by the side of one only with digital VCR by the side of one and cannot be displayed in digital VCR by the side of other.

[0089] Hereafter the copy prevention method of this invention and the flow of the MPEG bit stream by it are explained with reference to drawing 19 thru/or drawing 22.

[0090] Drawing 19 and 20 are the signal flow graphs to operation of a copy preventing process part at the time of record or reproduction mode Drawing 21 is a signal flow graph to operation of the smart card corresponding to said copy preventing process part and drawing 22 is a signal flow graph to record or the key exchange at the time of reproduction motion and an attestation process.

[0091] First the signal flow of drawing 19 is explained. The copy preventing process part 4 into which the bit stream was inputted checks the existence of key information distinguishes how of scrambling it has key information and when scramble is carried out it distinguishes whether it is the first recording or it is copy recording (S101).

[0092] Namely in the case of the data by which scramble was carried out it is searched whether it is transmitted by the stream of a $S_{KS}(BS)+IDX$ gestalt by separation of a bit stream ($S_{KS}(BS)$) and a key stream ($E^Q(KS)$) If the stream of a $S_{KS}(BS)+IDX$ gestalt is detected and it will distinguish from copy recording and will not be detected it distinguishes from the first recording (S102).

[0093] By this when distinguished from recording at first the stream ($S_{KS}(BS)+E^Q(KS)$) with which the bit stream and the key stream were mixed by VCR5 is recorded on a tape (S106) When distinguished from copy recording while a key stream ($E^Q(KS)$) transmits the separated bit stream ($S_{KS}(BS)+IDX$) to the copy preventing process part 8 by the side of record The key information A_k is received in said key stream ($E^Q(KS)$) After enciphering furthermore (S105) it will record on a tape by VCR9 by the side of record by transmitting the enciphered key stream ($E^{SO}_{AK}[E^Q(KS)]$) to the smart card 7 by the side of record via the smart card 3 (S106).

[0094] On the contrary drawing 20 is a signal flow graph in the case of playing the tape which recorded by a signal flow like drawing 19. The copy preventing process part 4 will distinguish whether (S108) and a recording function are "Back-up Copy" by separating and distinguishing a key stream when the bit stream reproduced with VCR is inputted (S107) (S110).

[0095] Under the present circumstances said stage (S110) will be distinguished from a recording tape at first if there is no key information it distinguishes from a common

recording tape and the enciphered key stream ($E^G(KS)$) is detected. If the key stream ($D^{SC}_{Ak}[E^G(KS)]$) decoded to the own key information Ak is detected, it distinguishes from the recording tape of a PPC function and if the key stream ($D^{SC}_{Al}[E^G(KS)]$) decoded to key information aluminum of other smart cards is detected, it will distinguish from the recording tape of the "Back-up Copy" function. By this, when general ** is a tape, the copy preventing process part 4. The bit stream ($S_{KS}(BS)+IDX$) from which the bit stream (BS) was separated in the key stream ($E^G(KS)$) in the case of the recording tape for copy prevention is transmitted to the decoder 2 (S109). [0096] And when a Back-up Copy function is applied to the copy preventing process part 4 at the time of playback of the recording tape for copy prevention, by enciphering twice by encryption algorithm $E^{SC}_{Ak}(-)$ to the own key information Ak, a key stream ($D^{SC}_{Ak}[E^G(KS)]$). The enciphered key stream ($E^{SC}_{Ak}[E^G(KS)]$) is transmitted to the smart card 3 (S111, S112, S113). When the Back-up Copy function is not applied, Keast RIMUMU ($E^G(KS)$) by enciphering by an encryption algorithm ($E^{SC}_{Ak}(-)$) to the own key information Ak. The enciphered key stream ($E^{SC}_{Ak}[E^G(KS)]$) is transmitted to the smart card 3 (S112, S113).

[0097] When performing the above operations in the copy preventing process part 4, the smart card 3 operates a signal flow like drawing 21. If this is explained in detail, said smart card 3 will distinguish whether the index code IDX or a key stream ($E^G(KS)$) is inputted by the decoder 2 by performing broadcast or reproduction (S114, S115).

[0098] Under the present circumstances, the smart card 3 distinguished from broadcast viewing and listening of the PPV function when the key stream ($E^G(KS)$) which is not the index code IDX was inputted. Said key stream ($E^G(KS)$) is decoded by decryption algorithm $D^G(-)$ to the bit stream GA (S116) and the key information KS is made to input into the decoder 2 (S117). By this, the decoder 2 deciphers the key information KS on the smart card 3 and distinguishes a descrambling method. By descrambling a bit stream ($S_{KS}(BS)$) and outputting as an analog video signal and an audio signal by the distinguished descrambling method, the televisioner can view and listen to broadcast. [0099] On the other hand, if it is distinguished that the index code IDX was inputted in said stage (S115), after the smart card 3 decodes the key stream ($E^{SC}_{Ak}[E^G(KS)]$) inputted in the copy preventing process part 4 with a decryption algorithm ($D^{SC}_{Ak}(-)$) to the key information Ak (S118), reproduction motion — or recording operation is distinguished (S119).

[0100] Under the present circumstances, if distinguished from reproduction motion in said stage (S119), the smart card 3 will decode the decrypted key stream ($E^G(KS)$) with the decryption algorithm ($D^G(-)$) to the bit stream GA (S116). The key information KS is made to input into the decoder 2 (S117). The decoder 2 deciphers the key information KS on the smart card 3 by this. Distinguish a descrambling method and the bit stream ($S_{KS}(BS)$) separated in the copy preventing process part 4 by the distinguished descrambling method is descrambled. By outputting an analog video signal

and an audio signal the televiewer can view and listen to the recording program of a tape.

[0101] And if distinguished from recording operation in said stage (S119) it will be distinguished whether the smart card 3 is the "Back-up Copy" function (S120). If it is the "Back-up Copy" function the key information A_k is received in a key stream ($E^G(KS)$). The key stream ($D^{SC_{A_k}}[E^G(KS)]$) (to key information aluminum) which decrypted with the decryption algorithm ($D^{SC_{A_k}}(-)$) (S121) and was decrypted. It will decrypt with a decryption algorithm ($D^{SC_{A_k}}(-)$) (S122).

[0102] Under the present circumstances the key stream ($D^{SC_{A_i}}[D^{SC_{A_k}}[E^G(KS)]]$) decrypted with the smart card 3 is transmitted to the record side (S123). If inputted into the copy preventing process part 8 via the smart card 7 (S124) it will be enciphered by an encryption algorithm ($E^{SC_{A_i}}(-)$). By this if the smart card 7 is mixed with the bit stream ($S_{KS}(BS)$) which made mix the enciphered key stream ($D^{SC_{A_k}}[E^G(KS)]$) in the position specified by the index code IDX and was outputted from the copy preventing process part 4 by the side of reproduction. It will record on a tape by VCR9.

[0103] On the other hand if it is distinguished from recording operation in said stage (S119) and it is distinguished that the PPC function which is not the "Back-up Copy" function in said stage (S120) was applied. The smart card 3 decrypts a key stream ($E^G(KS)$) with a decryption algorithm ($D^{SC_{A_i}}(-)$) to key information aluminum (S122). The decrypted key stream ($D^{SC_{A_i}}[E^G(KS)]$) will be transmitted to the record side (S123).

[0104] Under the present circumstances the copy preventing process part 8 by the side of the record which received the input of the key stream ($D^{SC_{A_i}}[E^G(KS)]$) via the smart card 7. After enciphering by encryption algorithm $E^{SC_{A_i}}(-)$ the enciphered key stream ($E^G(KS)$) will be made to mix in the position specified by the index code IDX and it will mix with the bit stream ($S_{KS}(BS)$) outputted from the copy preventing process part 4 by the side of reproduction.

[0105] Therefore the bit stream ($S_{KS}(BS) + E^G(KS)$) outputted from the copy preventing process part 8 is recorded on a tape by VCR9.

[0106] As mentioned above in this invention all the smart cards have a common algorithm and a common key to the encryption algorithm ($E^G(-)$) to an MPEG bit stream and a decryption algorithm ($D^G(-)$).

[0107] And although the encryption algorithm ($E^{SC_{A_i}}(-)$) to a smart card and a decryption algorithm ($D^{SC_{A_k}}(-)$) have an algorithm with all the common smart cards key information changes with smart cards. That is each smart card will contain the attestation key applicable to own recognition name ID.

[0108] In performing the above operations the processing-ized operation including the process in which the attestation process and key which can recognize a partner are exchanged is required between a copy preventing process part and between smart cards and smart cards. Under the present circumstances the method with various method of using a symmetrical key algorithm [like a DES algorithm] whose

attestation process is method of using a public key algorithm like RSA method of using FS (Fiat-Shamir) Scheme etc. is shown.

[0109] By this invention while performing the attestation process in which a public key algorithm was used the example of the method of exchanging keys was shown in drawing 22 but. Such a method is a basis of the premise that the key reception means 201 and the key transmission means 202 which are going to attest a public key (ne) are sharing and will be applied.

[0110] Under the present circumstances the key reception means 201 is the smart card 1 by the side of a copy preventing process part or record and the key transmission means 202 is the own smart card k.

[0111] Hereafter working example of this invention which operates by the above flows is described with reference to drawing 12 thru/or drawing 18.

[0112] Since the circuit operates as shown in drawing 12 when bit stream BS like drawing 11 (a) by which scramble is not carried out is transmitted in this invention analog video and an audio signal are outputted more for the bit stream by which strange recovery and RS decoding were carried out by the recovery and the error correcting section 1 to being decoded by the decoder 2.

[0113] Under the present circumstances bit stream BS which is outputted from a recovery and the error correcting section 1 in record it is recorded on a tape by VCR5 via the copy preventing process part 4 and in playback analog video and an audio signal are outputted by inputting into the decoder 2 bit stream BS played by VCR5 and decoding it via the copy preventing process part 4. That is since data is not outputted to the smart card 3 from the copy preventing process part 4 viewing and listening and a copy are not affected.

[0114] And when drawing 11 (b) or the bit stream by which scramble was carried out as shown in (c) enters in drawing 13 operation like drawing 18 is performed by applying CA function.

[0115] First when performing a PPV function operate by a signal flow like drawing 13 but. If the key stream (E^G (KS)) enciphered as the bit stream (S_{KS} (BS)) by which scramble was carried out is transmitted a recovery and the error correcting section 1 will correct the error generated during transmission via RS decoding after restoring to the modulated input signal.

[0116] Under the present circumstances if the decoder 2 separates a key stream (E^G (KS)) among a recovery and the output (S_{KS} (BS) + E^G (KS)) of the error correcting section 1 and outputs to the smart card 3 The smart card 3 decodes said enciphered key stream (E^G (KS)) and outputs the key stream KS to said decoder 2 further. By this after the decoder 2 deciphers the key stream KS of the smart card 3 and distinguishes a descrambling method it will decode a bit stream (S_{KS} (BS)) and will output an analog video signal and an audio signal.

[0117] Here the processor 11 will decode the key stream (E^G (KS)) enciphered with the decryption algorithm (E^G (-)) and the smart card 3 like drawing 9 will output the

decoded key stream KS to the decoder 2.

[0118]On the other handwhen recording first the bit stream by which scramble was carried outoperate by a signal flow like drawing 14but. After an error is corrected via a recovery and RS decoding by a recovery and the error correcting section 1 the transmitted bit stream ($S_{KS}(BS)+E^G(KS)$) is inputted into VCR5 via the copy preventing process part 4 and is recorded on a tape.

[0119]When playing the bit stream recorded in this way and it is a PPP function operate by a signal flow like drawing 15 but. If the bit stream ($S_{KS}(BS)+E^G(KS)$) reproduced by VCR5 is inputted into the copy preventing process part 4 After the copy preventing process part 4 divides the reproduced bit stream ($S_{KS}(BS)+E^G(KS)$) into a bit stream ($S_{KS}(BS)$) and a key stream ($E^G(KS)$) Said separated key stream ($E^G(KS)$) is further enciphered by an encryption algorithm ($E^{SC}_{AK}(-)$) It outputs to the smart card 3 and said separated bit stream ($S_{KS}(BS)$) carries out load of the index code IDX to the portion from which the key stream ($E^G(KS)$) was taken out and outputs it to the decoder 2.

[0120]Under the present circumstances the smart card 3 which received the input of the index code IDX via the decoder 2 The key stream ($E^{SC}_{AK}[E^G(KS)]$) as which the copy preventing process part 2 was enciphered is decoded with the decryption algorithm ($D^{SC}_{AK}(-)$) for a smart card The key stream KS which is descrambling information is outputted to said decoder 2 (S117). After the decoder's 2 deciphering the key stream KS of the smart card 3 and distinguishing a descrambling method by this By decoding the bit stream ($S_{KS}(BS)$) inputted via the copy preventing process part 4 an analog video signal and an audio signal will be outputted.

[0121]And when recording the data recorded by a signal flow like drawing 14 with different VCR perform a PPC function like the signal flow of drawing 16 but. When the bit stream ($S_{KS}(BS)+E^G(KS)$) reproduced by VCR5 is inputted into the copy preventing process part 4 the copy preventing process part 4 A bit stream ($S_{KS}(BS)+E^G(KS)$) is divided into a bit stream ($S_{KS}(BS)$) and a key stream ($E^G(KS)$). Then encipher said separated key stream further by an encryption algorithm ($E^{SC}_{AK}(-)$) and it outputs to the smart card 3 The index code IDX will be added to the portion from which said separated bit stream ($S_{KS}(BS)$) and the key stream ($E^G(KS)$) were taken out and it will output to the copy preventing process part 8 by the side of record.

[0122]Under the present circumstances after the smart card 3 by the side of reproduction decodes the key stream ($E^{SC}_{AK}[E^G(KS)]$) enciphered in the copy preventing process part 4 with a decryption algorithm ($D^{SC}_{AK}(-)$) to key information aluminum stored in RAM The decoded key stream ($D^{SC}_{AK}[E^G(KS)]$) will be outputted to the smart card 7 by the side of record. By this if the smart card 7 by the side of record outputs to the copy preventing process part 8 by the side of record in response to the input of the key stream ($D^{SC}_{AK}[E^G(KS)]$) of the smart card 3 by the side of reproduction After said copy preventing process part's 8 enciphering said key stream ($D^{SC}_{AK}[E^G(KS)]$) and restoring to the enciphered original key stream (E^G

(KS))By mixing to the bit stream ($G_{KS}(BS)$) outputted from the copy preventing process part 4 by the side of playbackand outputting to VCR5 by the index code IDXit will record on other tapes.

[0123]The data of the tape recorded in such operation can apply a PPP functionand can play it by a signal flow like drawing 15. When recording the data recorded by a signal flow like drawing 14 with other VCRa Back-upCopy function can be performed like the signal flow of drawing 17.

[0124]That is if the bit stream ($S_{KS}(BS)+E^G(KS)$) reproduced by VCR5 is inputted into the copy preventing process part 4After dividing the copy preventing process part 4 into a bit stream ($S_{KS}(BS)$) and a key stream ($E^G(KS)$)Encipher said separated key stream further by an encryption algorithm ($E^{SC}_{AK}(-)$)and it outputs to the smart card 3Said separated bit stream ($S_{KS}(BS)$) will add the index code IDX to the portion from which the key stream ($E^G(KS)$) was taken outand will output it to the copy preventing process part 8 by the side of record.

[0125]Under the present circumstancesafter the smart card 3 by the side of reproduction decrypts twice the key stream ($E^{SC}_{AK}[E^G(KS)]$) enciphered in the copy preventing process part 4 with a decryption algorithm ($D^{SC}_{AK}(-)$) to the key A_k of the self stored in ROMIt decodes with a decryption algorithm ($D^{SC}_{AI}(-)$) to key information aluminum furthermore stored in RAMThe decoded key stream ($D^{SC}_{AI}[D^{SC}_{AK}[E^G(KS)]]$) will be outputted to the smart card 7 by the side of record. By this if the key stream ($D^{SC}_{AI}[D^{SC}_{AK}[E^G(KS)]]$) of the smart card 3 by the side of reproduction is outputted to the copy preventing process part 8 by the side of record via the smart card 7 by the side of recordBy enciphering to key information aluminumthe copy preventing process part 8 restores said key stream ($D^{SC}_{AI}[D^{SC}_{AK}[E^G(KS)]]$) to the original cryptographic key stream ($D^{SC}_{AK}[E^G(KS)]$). And the restored cryptographic key stream ($D^{SC}_{AK}[E^G(KS)]$)By the index code IDXit will mix to the bit stream ($G_{KS}(BS)$) outputted from the copy preventing process part 4 by the side of playbackwill output to VCR9and will record on other tapes.

[0126]Herea fee is calculated by the improved smart card 3 or 7.

[0127]Although the data recorded by performing such a Back-up Copy function is renewable only with VCR which recorded the former tapewhen it is normal playbackit operates by a signal flow like drawing 18 (a).

[0128]That is if the bit stream ($S_{KS}(BS)+D^{SC}_{AK}[E^G(KS)]$) reproduced by VCR5 is inputted into the copy preventing process part 4The copy preventing process part 4 is divided into a bit stream ($S_{KS}(BS)$) and a key stream ($D^{SC}_{AK}[E^G(KS)]$). Thensaid separated key stream ($D^{SC}_{AK}[E^G(KS)]$) is enciphered twice by an encryption algorithm ($E^{SC}_{AK}(-)$)It outputs to the smart card 3and said separated bit stream ($S_{KS}(BS)$) adds the index code IDX to the portion from which the key stream ($D^{SC}_{AK}[E^G(KS)]$) was taken outand outputs it to it to the decoder 2.

[0129]In this case. Via the decoder 2. The smart code 3 which received the input of the index code IDX decodes the key stream ($E^{SC}_{AK}[E^G(KS)]$) enciphered in the copy

preventing process part 2 with the decryption algorithm ($D_{AK}^{SC}(-)$) for a smart card. The key stream KS which is descrambling information is outputted to said decoder 2. After the decoder's 2 deciphering the key stream KS of the smart card 3 and distinguishing a descrambling method by this. By decoding the bit stream ($S_{KS}(BS)$) inputted via the copy preventing process part 4, an analog video signal and an audio signal will be outputted.

[0130] And in the abnormal playback played with other VCR which is not VCR recorded at first, it will operate by a signal flow like drawing 18 (b) and playback of a tape becomes impossible.

[0131] That is, if a copy tape is played by VCR 9 which performed the tape copy splitting processing of the data ($S_{KS}(BS) + D_{AK}^{SC}[E^G(KS)]$) played in the copy preventing process part 8, it will be carried out. A bit stream ($S_{KS}(BS) + IDX$) is separated.

[0132] Under the present circumstances, after the separated key stream ($D_{AK}^{SC}[E^G(KS)]$) was enciphered to own key information aluminum. Furthermore, it is enciphered to key information aluminum ($E_{AI}^{SC}[E_{AI}^{SC}(D_{AK}^{SC}[E^G(KS)])]$) and is transmitted to the smart card 7. And since the smart card 7 cannot decode a bit stream ($E_{AI}^{SC}[E_{AI}^{SC}(D_{AK}^{SC}[E^G(KS)])]$), the key information KS is not transmitted to the decoder 6. Therefore, since the smart card 7 does not descramble a bit stream ($S_{KS}(BS)$), playback of a copy tape is not performed.

[0133] On the other hand, it is as follows when the term used for this invention for the understanding of this invention is defined.

[0134] 1) GA bit stream $2KS = [$ which is not carried out as for BS: scramble — $K_0, K_1, K_2, \dots, K_i$ and $\dots, K_n]$: key stream — here, total $3BS = [$ of the key by which n was used for scrambling — $BS_0, BS_1, BS_2, \dots, BS_n]$: bit stream — here, Unit $4S_{KS}(BS)$ which carries out the scramble of the BS_i as one segment of BS : MPEG bit stream $S_{KS}(BS) = [SK_0$ by which scramble was carried out (BS_0), $SK_1(BS_1), \dots, SK_i(BS_i)$ and \dots algorithm $E^G(KS)$ used for enciphering and decrypting a key by $SK_n(BS_n)]$ 5E&D (and): $GA = [E^G(K_0)$ and $E^G(K_1), \dots, E^G(K_i), \dots, E^G(K_n)]$ $D^G(KS) = [D^G(K_0)$ $D^G(K_1), \dots, D^G(K_i), \dots, D^G(K_n)] = KS6IDX: [01$ and $2, \dots, i, \dots, n]$: index stream 7Ak: — attestation key $8E_{AK}^{SC}(-) [\& D_{AK}^{SC}(-)$: of a smart card (A) — encryption and the decryption algorithm of the smart card which used the attestation

key (A) of the smart card as the key.

[0135]

[Effect of the Invention] Since this invention performs attestation and a key exchange process automatically at the time of power-on or connection between digital VCR as explained above. Since illegal viewing and listening to an illegal smart card and a copy preventing function can be performed automatically and illegal viewing and listening and prevention from a copy can be performed still more nearly selectively. If scrambling processing is performed into the portion which wishes protection of a program fee, can also be imposed as a request performing illegal viewing and listening and prevention from a copy automatically.

[0136] And since this invention transmits a bit stream and the key stream made to separate in a differing course. When the quantity of protected data can be decreased and illegal viewing and listening and a copy preventing function can be performed efficiently and the prevention from illegal viewing and listening and an illegal copy preventing function are embodied to a smart card, a fee can be discriminatorily imposed to each function by distinguishing PPVPPPP and a Back-up Copy function.

[0137] This invention is applicable to the copyright-to-program protection in DSM like digital VCR by embodying the copy preventing function of the digital signal which can be applied to DSM application. Therefore application of this invention will acquire the effect that the reliability over illegal viewing and listening and the prevention from a copy can be raised.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram of a general scrambler.

[Drawing 2] It is a block diagram of a general descrambler.

[Drawing 3] It is an illustration figure of a transmission format.

[Drawing 4] It is a detailed illustration figure of the PES header in drawing 3.

[Drawing 5] It is an illustration figure of the transmission format by key distribution.

[Drawing 6] It is a block diagram of the conventional ATV decoder.

[Drawing 7] They are illegal viewing and listening of this invention and a block diagram of a copy arrester.

[Drawing 8] It is a detailed block diagram of the copy preventing process part in drawing 7.

[Drawing 9] It is a detailed block diagram of the smart card in drawing 7.

[Drawing 10] It is an illustration figure showing the splitting (splitting) of the bit stream in drawing 8.

[Drawing 11] (a) ~ (f) is an illustration figure showing the format of each bit stream.

[Drawing 12] It is an illustration figure showing the connected state of this invention.

[Drawing 13] It is an illustration figure showing the connected state of this invention.

[Drawing 14] It is an illustration figure showing the connected state of this invention.

[Drawing 15] It is an illustration figure showing the connected state of this invention.

[Drawing 16] It is an illustration figure showing the connected state of this invention.

[Drawing 17] It is an illustration figure showing the connected state of this invention.

[Drawing 18] It is an illustration figure showing the connected state of this invention.

[Drawing 19] It is a signal flow graph for operation of this invention.

[Drawing 20] It is a signal flow graph for operation of this invention.

[Drawing 21] It is a signal flow graph for operation of this invention.

[Drawing 22] It is a signal flow graph for the key exchange by this invention and an attestation process.

[Description of Notations]

1 and 104 A recovery and error correcting section

26 ATV decoder

3 Smart card

4 and 8 Copy preventing process part

11 and 18 Processor

【特許請求の範囲】

【請求項 1】 入力されるデータがスクランブル(scramble)されたかどうかを判別する判別段階と、

前記判別段階でスクランブルされたデータと判別されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、キー情報に応じて前記分離されたビットストリームをデスクランブル(descramble)して、ディスプレイ装置にディスプレイする再生段階と、

前記判別段階でスクランブルされたデータと判別されると、記録もしくは複写モードに応じて、ビットストリームとキーストリームが混合されたスクランブルされたデータ状態で記録媒体に記録したり、スクランブルされたデータをビットストリームとキーストリームに分離し、分離されたキーストリームを暗号化した後、ビットストリームと混合して記録媒体に記録する記録段階と、前記判別段階でスクランブルされたデータと判別されると、スクランブルされたデータをビットストリームとキーストリームに分離した後、「PPC」モードもしくは「バックアップ・コピー(Back-up Copy)」モードに応じて分離されたキーストリームを記録側のキー情報に対して復号化して伝送したり、分離されたキーストリームを自身のキー情報と記録側のキー情報に対して 2 回復号化して伝送する伝送段階とからなり、

前記再生段階、記録段階、伝送段階は、同時又は選択的に行うことができることを特徴とするデジタル映像システムの不法視聴及び複写防止方法。

【請求項 2】 前記判別段階でスクランブルされていないデータと判別されると、スクランブルされていないデータは不法視聴及び複写防止機能を用いないことを特徴とする請求項 1 記載のデジタル映像システムの不法視聴及び複写防止方法。

【請求項 3】 前記再生段階は、分離されたキーストリームを MPEG ビットストリームに対する復号化アルゴリズムで復号化して、キー情報を判読することと特徴とする請求項 1 記載のデジタル映像システムの不法視聴及び複写防止方法。

【請求項 4】 前記記録段階の複写動作は、キーストリームを自身のキー情報に対して暗号化する第 1 段階と、第 1 段階で暗号化されたキーストリームが「PPC」モードであるか、或いは「バックアップ・コピー」モードであるかを判別する第 2 段階と、

前記第 2 段階で「PPC」モードと判別されると、記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第 3 段階と、

前記第 2 段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して

復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化し、その自身のキー情報に対して復号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第 4 段階とからなることを特徴とする請求項 1 記載のデジタル映像システムの不法視聴及び複写防止方法。

【請求項 5】 前記第 3 段階の「PPC」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第 1 伝送段階と、前記第 1 伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、記録側のキー情報に対して復号化して伝送する第 2 伝送段階と、前記第 2 伝送段階で伝送されたキーストリームをインデックスコードに対応して記録側のキー情報に対して暗号化した後、前記第 1 伝送段階で伝送されたビットストリームに混合して記録媒体に記録する記録段階とからなることを特徴とする請求項 4 記載のデジタル映像システムの不法視聴及び複写防止方法。

【請求項 6】 前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+E^6(KS)$)をビットストリーム($S_{KS}(BS)$)とキーストリーム($E^6(KS)$)に分離した後、キーストリーム($E^6(KS)$)が分離された部分にインデックスコード I DX を挿入する第 1 分離段階と、前記分離段階で分離されたキーストリーム($E^6(KS)$)を自身のキー情報に対して暗号化する暗号化段階と、前記暗号化段階で暗号化されたキーストリームを自身のキー情報と MPEG ビットストリームに対して復号化することによりキー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて前記分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルする復号化段階とを含むことを特徴とする請求項 5 記載のデジタル映像システムの不法視聴及び複写防止方法。

【請求項 7】 前記第 4 段階の「バックアップ・コピー」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第 1 伝送段階と、

前記第 1 伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、暗号化されたキーストリームを記録側のキー情報と自身のキー情報に対して復号化して伝送する第 2 伝送段階と、前記第 2 伝送段階で伝送されたキーストリームをインデックスコードに対応して、記録側のキー情報に対して暗号化した後、前記第 1 伝送段階で伝送されたビットストリームに混合して、記録媒体に記録する記録段階とからなることを特徴とする請求項 4 記載のデジタル映像システムの不法視聴及び複写防止方法。

【請求項 8】 前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+D^{SC}AK$)

6(KS))を、ビットストリーム(S_{KS}(BS))とキーストリーム(D_{SK}AK[E₆(KS)])を分離した後、キーストリーム(D_{SK}AK[E₆(KS)])が分離された部分に、インデックスコードID_Xを挿入する分離段階と、

前記分離段階で分離されたキーストリーム(D_{SK}AK[E₆(KS)])を自身のキー情報に対して暗号化する暗号化段階と、

前記暗号化段階において、2回暗号化されたキーストリームを自身のキー情報とMPEGビットストリームに対して復号化することにより、キー情報を判読する判読段階と、

前記判読段階で判読されたキー情報に基づいて、分離されたビットストリーム(S_{KS}(BS))をデスクランブルする復号化段階とを含むことを特徴とする請求項7記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項9】 スクランブルされたデータが入力されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号しキー情報を判読し、判読されたキー情報に基づいて、前記分離されたビットストリームをデスクランブルして、ディスプレイ装置にディスプレイする再生段階と、

スクランブルされたデータが入力されると、ビットストリームとキーストリームが混合されたスクランブルされたデータ状態で、記録媒体に記録する記録段階とからなり、

前記再生段階、記録段階は、同時若しくは選択的に行うことができることを特徴とするディジタル映像システムの不法視聴及び複写防止方法。

【請求項10】 前記再生段階は、分離されたキーストリームを、MPEGビットストリームに対する復号化アルゴリズムで復号してキー情報を判読し、判読されたキー情報で、デスクランブル方式を判別することと特徴とする請求項9記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項11】 前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム(S_{KS}(BS)+E₆(KS))をビットストリーム(S_{KS}(BS))とキーストリーム(E₆(KS))に分離した後、キーストリーム(E₆(KS))が分離された部分に、インデックスコードID_Xを挿入する分離段階と、前記分離段階で分離されたキーストリーム(E₆(KS))を自身のキー情報に対して、暗号化アルゴリズムで暗号化する暗号化段階と、

前記暗号化段階で2回暗号化されたキーストリームを、自身のキー情報とMPEGビットストリームに対して復号化することにより、キー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて、前記分離されたビットストリーム(S_{KS}(BS))をデスクランブルして、ディスプレイ装置にディスプレイする復号化段階

と、を含むことを特徴とする請求項9記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項12】 複写時に自身のキー情報に対して暗号化されたキーストリームが伝送されると、「バックアップ・コピー」モードであるか、もしくは「PPC」モードであるかを判別する判別段階と、

前記判別段階で「PPC」モードと判別されると、記録側のキー情報に対して前記キーストリームを復号化して伝送する第1伝送段階と、

前記第1伝送段階で伝送されたキーストリームを記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入して、ビットストリームのように記録媒体に記録する第1記録段階と、

前記判別段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して、キーストリームを2回復号化して伝送する第2伝送段階と、

前記第2伝送段階で伝送されたキーストリームを、記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入してビットストリームのように記録媒体に記録する第2記録段階と、からなることを特徴とするディジタル映像システムの不法視聴及び複写防止方法。

【請求項13】 前記第1伝送段階は、自身のキー情報A_kに対して暗号化されたキーストリームを自身のキー情報A_kに対して復号化し、さらに記録側のキー情報A_lに対して復号化した後、伝送することと特徴とする請求項12記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項14】 前記第2伝送段階は、自身のキー情報A_kに対して暗号化されたキーストリームを、自身のキー情報A_kに対して2回復号化し、さらに記録側のキー情報A_lに対して復号化した後伝送することと特徴とする請求項12記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項15】 記録媒体の再生時にキーストリーム(E₆(KS))が検出されると「PPC」記録媒体と判別して、キーストリームを自身のキー情報に対して暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いて、ビットストリームをデスクランブルする「PPC」モード再生段階と、

記録媒体の再生時に自身のキー情報に対して復号化されたキーストリーム(D_{SK}AK[E₆(KS)])が検出されると、「バックアップ・コピー」記録媒体と判別して、自身と記録側のキー情報に対して2回暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いてビットストリームをデスクランブルする「バックアップ・コピー」モード再生

段階とかなることを特徴とするデジタル映像システムの不法視聴及び複写防止方法。

【請求項16】 アナログ放送信号を変復調してRSデコードする復調及び誤り訂正手段と、

前記復調及び誤り訂正手段の出力を記録／再生装置に伝送し、その記録／再生装置で再生されるスクランブルされた記録信号をビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する複写防止処理手段と、

前記復調及び誤り訂正手段若しくは複写防止処理手段から出力されるビットストリームをデスクランプリング情報に基づいてデスクランブルするデコーダ手段と、
前記複写防止処理手段で暗号化されたキーストリームを復号して、前記デコーダ手段へデスクランプリング情報として出力するスマート手段とから構成したことを特徴とするデジタル映像システムの不法視聴及び複写防止装置。

【請求項17】 前記復調及び誤り訂正手段が接続されたデコーダ手段をスマート手段に接続して、前記スマートカードで前記デコーダ手段のキーストリームを自身のキー情報で復号して、デスクランプリング情報を前記デコーダ手段へ出力することにより、不法視聴防止機能を行うように構成したことを特徴とする請求項16記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項18】 前記復調及び誤り訂正手段が接続された複写防止処理手段を、デジタル記録／再生装置に接続して初めて録画を行うことを特徴とする請求項16記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項19】 前記デジタル記録／再生装置が接続された複写防止手段のキーストリームラインを、スマートカードに接続するとともに、ビットストリームラインをデコーダ手段に接続し、前記複写防止処理手段とデコーダ手段を接続して、前記スマートカードが前記デコーダ手段のインデックスコードに対応する前記複写防止処理手段のキーストリームを自身のキー情報で復号して前記デコーダ手段へ出力することにより不法再生を防止することを特徴とする請求項16記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項20】 前記複写防止処理手段は「PPC」モードの記録媒体再生時にデジタル記録／再生装置の再生データから分離したキーストリームを自身のキー情報で暗号化してスマートカードへ伝送することを特徴とする請求項19記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項21】 前記複写防止処理手段は、「バックアップ・コピー」モードの再生媒体再生時にデジタル記録／再生装置の再生データから分離したキーストリームを、自身のキー情報で2回暗号化してスマートカードへ伝送すること、を特徴とする請求項19記載のディジ

タル映像システムの不法視聴及び複写防止装置。

【請求項22】 前記複写防止処理手段は、スマートカード固有のキー情報を記憶するRAMと、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、
前記RAMのキー情報で前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセスとからなることを特徴とする請求項16、18、又は請求項19のいずれかに記載するデジタル映像システム及び複写防止装置。

【請求項23】 前記スマートカードは、ビットストリームの為の復号化アルゴリズムプログラムを貯蔵する第1アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第2アルゴリズム貯蔵メモリと、
自身のキー情報を貯蔵するROMと、
他のスマートカードのキー情報を一時貯蔵するRAMとから構成したことを特徴とする請求項16、17、又は請求項19のいずれかに記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項24】 第1デジタル記録／再生装置の再生データをビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する第1複写防止処理手段と、

前記第1複写防止処理手段で暗号化されたキーストリームを自身のキー情報と記録側のキー情報に対して復号化する第1、第2スマートカードと、
前記第2スマートカードを介して伝送された前記第1スマートカードのキーストリームを自身のキー情報で暗号化した後、暗号化されたキーストリームを分離されたビットストリームとともに、第2デジタル記録／再生装置へ出力して、記録媒体に記録する第2複写防止処理手段と、から構成したことを特徴とするデジタル映像システムの不法視聴及び複写防止装置。

【請求項25】 前記第1複写防止処理手段は、キーストリームを自身のキー情報Aに対して暗号化した後、第1スマートカードへ伝送すること、を特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項26】 前記第1スマートカードは、「PPC」モードである時、第1複写防止処理手段のキーストリームを自身のキー情報と記録側のキー情報に対して復号化した後、第2スマートカードへ伝送すること、を特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項27】 前記第2複写防止処理手段は、第2スマートカードで伝送されるキーストリームを自身のキー情報A1に対して暗号化した後、第1複写防止処理手段のビットストリームと混合すること、を特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写

防止装置。

【請求項28】 前記第1スマートカードは「バックアップ・コピー」モードであるとき、第1複写防止処理手段のキーストリームを自身のキー情報に対して2回復号した後、記録側のキー情報に対して復号することと特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項29】 前記第2複写防止処理手段は、第2スマートカードから伝送されるキーストリームを自身のキー情報に対して暗号化し、その暗号化されたキーストリームをビットストリームと混合することと特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項30】 前記第1、第2複写防止処理手段は、スマートカード固有のキー情報を貯蔵するRAMと、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、前記RAMのキー情報によって、前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサと、から構成したことを特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写防止装置。

【請求項31】 前記第1、第2スマートカードは、ビットストリームのための復号化アルゴリズムプログラムを貯蔵する第1アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第2アルゴリズム貯蔵メモリと、自身のキー情報を貯蔵するROMと、他のスマートキー情報を一時貯蔵するRAMとから構成したことを特徴とする請求項24記載のデジタル映像システムの不法視聴及び複写防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はデジタル映像システムの不法視聴及び複写防止技術に関する。特にスマートカードを導入して分離されたキーストリームを復号してデスクランプリング方式を設定するようにすることにより、無断使用者の不法視聴及び複写を防止するデジタル映像システムの不法視聴／複写防止方法及び装置に関する。

【0002】

【従来の技術】 一般的なデジタル映像システムで不法視聴防止のためにConditional Access（以下、CAという）システムの具現に関心が集中している。

【0003】 このようなCAシステムは、ケーブルTVや衛星放送などの有料チャンネルで放送信号をスクランブルされた形態で放送することにより、正式で金を払った使用者だけがデスクランプリングを介して際に放送プログラムを視聴し得るようにするものである。たとえば、衛星放送受信機若しくは米国A/T規格のGrandAlliance（以下、GAという）システムは、CAを支援

するための機能を持っており、G1社のビデオ暗号(Video Cipher)のような衛星放送に使用されるスクランプリング／デスクランプリング装置も既に常用化された。

【0004】 一般的なCAシステムのためのスクランプリングシステムは、G1社のビデオ暗号(Video Cipher)システムであり、G1HousenのU.S. Pat. No. 4613901特許を基礎とし、これは有料TVシステムで正規加入者のデスクランブラへ伝送されるTV信号をスクランブルして放送すると、正規加入者のデスクランブラで選択的にデスクランブルするシステム及び方法である。

【0005】 そして、デスクランプリングを行うビデオ暗号(Video Cipher)システムにスマートカードを導入して具現したものがU.S. Pat. No. 5111504であり、これはG1Housenのシステムをデスクランブラに該当する「情報プロセッサ(Information Processor)」と「スマートコード(smart card)」のように代替可能な「保護エレメント(Security Element)」に2分割して具現したものである。

【0006】 従って、前記方式を適用してスクランプリングシステムを図1のように具現すると、デスクランプリングシステムは図2のように具現される。

【0007】 即ち、従来のデジタル映像システムの不法視聴防止装置は、一般規格情報(Common Category Key) C K及び初期化ベクトル(Initialization Vector) P Kに応じてTV信号V i をスクランブルして、スクランブルされたTV信号S V oとスクランプリング情報(E U(D) E U(S) (CK), E K(PK))を出力するスクランブラ101と、デスクランプリングのための情報(A(D), A(S))をデスクランプリング情報(U(S))に対して暗号化(Encryption)するスマートカード103と、このスマートカード103のデスクランプリングのための情報(EA(D) [EA(S) (WK)])を復号(Decryption)して前記スクランブラ101の伝送TV信号S V oをデスクランブルすることにより元のTV信号D V oに復元する情報プロセッサ102とから構成される。ここで、A(D)は情報プロセッサ102の認証キー(Authentication Key)であり、A(S)はスマートカード103の認証キーであり、U(D)は前記情報プロセッサ102のユニットキー(Unit Key)であり、U(S)は前記スマートカード103のユニットキーである。

【0008】 この際、前記スクランブラ101は一般キーC Kをデスクランプリングのための情報(U(D) U(S))に対して暗号化する第1暗号化器111と、初期化ベクトルP Kを一般キーC Kに対して暗号化する第2暗号化器112と、初期化ベクトルP Kを前記第2暗号化器112の出力E K(PK)に対して暗号化する第3暗号化器113と、TV信号V i を前記第3暗号化器113の出力WKに応じてスクランブルするスクランプリング遂行端114とから構成される。

【0009】 以下、このように構成された従来装置の動作過程を説明する。

【0010】まず、伝送システムでTV信号を伝送しようとする場合、スクランブラ101は第1暗号化器111で一般規格情報(Common Category Key)CKをデスクランプリングのための情報(U(0))、(U(S))に対して暗号化し、第2暗号化112で初期化ベクトル情報(Initialization Vector)PKを一般規格情報CKに対して暗号化し、第3暗号化器113で初期化ベクトル情報PKを前記第2暗号化器112の出力(E_{CK}(PK))に対して暗号化してスクランプリング処理端114へ出力する。この際、スクランプリング処理端114は第3暗号器113の出力WKを基準としてTV信号Viをスクランブルする。ここで、スクランプリング情報WKはE_{CK}(PK)(PK)で表れる。

【0011】これにより、スクランブラ101は一般規格情報CKに対する暗号化情報(E_U(0))E_U(S)(CK)、初期化ベクトル情報PKに対する暗号化情報(E_{CK}(PK))及びスクランブルされたTV信号SVoを情報プロセッサ102へ伝送することになる。

【0012】一方、スクランブルされたTV信号SVoをデスクランブルする場合、スマートカード103は情報プロセッサ102の認証情報(A(D))と自身の認証情報(A(S))に対してデスクランプリングに必要な情報WKを暗号化した後、その暗号化されたデスクランプリング情報(E_A(D)[E_A(S)(WK)])を情報プロセッサ102へ出力する。

【0013】これにより、情報プロセッサ102はスマートカード103から出力された暗号化された情報(E_A(D)[E_A(S)(WK)])を復号し、これを用いてスクランブラ101から伝送されたTV信号SVoをデスクランブルすることによって元のTV信号Voに復元することになる。

【0014】ここで、情報プロセッサ102とスマートカード103間の情報伝送に暗号化(Encryption)を適用することは、不法視聴及び複写から保安性を高めるためのものである。

【0015】例えば、GA(Grand Alliance)高画質TVシステムの内訳(spec.)はC Aシステムを支援し、且つ伝送プロトコルに必要な機能が具現されている。このシステムに具現された機能は、使用可能な全てのデスクランプリング方法及びキー暗号化(Key Encryption)方法を支援するという意味において、フレキシブル(Flexible)であり、有用であり、且つビットストリームを選択的にスクランブルすることができて、エレメントストリーム単位でC A機能を適用し得る融通性(Flexibility)が保障される。ここで、スクランプリングは、情報データに基づいて、データビットストリームを不規則(Random)にすることを意味し、暗号化(Encryption)する不法使用者から情報データを保護するために変換する過程を意味する。つまり、C Aシステムは伝送されるデータをスクランブラを用いて不規則にして、TV放送を無断で視聴し

ようとする不法使用者側のデコーダは確にデコードできないようにする一方、TV放送が許可された使用者側のデコーダはデスクランブラ回路をフォーマットする情報を提供して受信されたTV放送信号を正常的にデコードし得るようにするものである。

【0016】前記動作のためのMPEGの伝送プロトコルは、図3のようなフォーマットで具現することができ、このような伝送プロトコルはC A機能を支援する2つの特性がある。

【0017】第1、2ビットのTransport-scrambling-controlフィールドは、伝送ストリームがスクランブルされたかどうかと、スクランブルされた場合にどんなスクランプリングキーが使用されたかを知らせてくれる。

【0018】第2、伝送ストリームの適応(Adaptation)ヘッダ内のTransport-private-dateフィールドを用いて個々のデータをGA伝送システム内に挿入する機能で、このようなフィールドには暗号化されたスクランプリング情報を貯蔵する。

【0019】前記特性を有する図3のようなMPEGの伝送プロトコルは、伝送ヘッダ、PES(Packetized Elementary Stream)ヘッダ、そして引き続きオーディオ及びビデオデータをそれぞれ若しくは同時に伝送するが、伝送ヘッダはリンクヘッダ(Link Header)、適応ヘッダ、及びプレイロード(playload)領域から構成される。

【0020】ここで、リンクヘッダ(Link header)は4バイトの長さ、適応ヘッダは可変的な長さを有する。

【0021】前記リンクヘッダには、Transport-scrambling-controlフィールドが挿入され、このフィールドの値は「00」であればNot-Scrambled、「10」であればEvenキー、「11」であればOddキー、「01」であればReservedと認識することになる。

【0022】そして、適応ヘッダにはフラグビットとTransport-private-dataフィールドが含まれ、前記フラグビット中には1ビットのTransport-private-dataフラグを含む。尚、図3のようなMPEGの伝送プロトコルのPESヘッダは図4のように構成される。

【0023】このPESヘッダにはデジタルVCRのようなデジタル記憶媒体DSMのためのフィールドが存在するが、このようなフィールドは14ビットの長さを有するPESヘッダフラグ領域と可変長さを有するPESヘッダフィールドを含んで構成される。

【0024】前記PESヘッダフラグ領域には1ビットのCR(Copyright)フラグ、1ビットのOC(original-or-copy)フラグ、2ビットのPDフラグ、1ビットのTMフラグ、そして1ビットのACフラグを含んで構成する。

【0025】そして、PESヘッダフィールドは可変的な長さを有し、PESヘッダフラグ領域に含まれたPD、TM、ACフラグによって一部領域が設定される。即ち、PESヘッダフラグでPTS/DTS領域は、PD

フラグの値が「00」であれば存在せず、「10」であれば40ビット、「11」であれば80ビットとなり、DSM Trick ModeフィールドはTMフラグの値が「0」であれば存在せず、「1」であれば8ビットとなり、Additional Copy Info. フィールドはACフラグが「1」とセットされるとき、8ビットとなっているべきである。

【0026】このようなフォーマットを適用することにより、スクランプリング情報を伝送し、この情報を用いてデスクランプリングする過程を図5に示した。

【0027】ここで、デスクランプリングシステムは、現在デスクランプリングに使用されているキーとともに、次の暗号化されたキーが復号されているべきであって、デスクランプリングは「Oddキー」と「Evenキー」のふたつを貯蔵していなければならない。そして、スクランプリングシステムは、現在の伝送ストリームがデスクランプリングされる方式によって、リンクヘッダ内のtransport-scrambling-controlフィールドの値をセットして伝送しなければならない。

【0028】これにより、デスクランプリングは受信データで復号された伝送ヘッダのTransport-scrambling-controlフィールドの値によって「Even or Odd」キーを判別した後、受信データをデスクランプリングして復号することになる。

【0029】即ち、図5のようなフォーマットのデータが伝送されて、スマートカードで復号されたTransport-scrambling-controlフィールドの値によって、デスクランプリングがK_{2n}-番目のフレームをOddキーでデスクランプリングしているとき、スマートカードは次にデスクランプリングするK_{2n}番目のフレームでTransport-scrambling-controlフィールドを復号し、このような動作は順次行われる。

【0030】一方、CA機能を行うATVデコーダを例え図6のように実現することができるが、このようなATVデコーダ110は伝送デマルチプレクサ105に高速演算が必要なデスクランプリングを内蔵してDESアルゴリズムやPNシーケンスを用いたストリームサイバークリプター(cipher)アルゴリズム等でデスクランプリングを行うことになり、このATVデコーダ110で暗号化されたキー(Encrypted Key)はスマートカード103で復号化(Decryption)される。

【0031】ここで、スマートカード103とATVデコーダ110のインタフェースはISO-7816標準規格等によってなされる。

【0032】即ち、図6の実施例はチューナで受信された信号が復調及び誤り訂正部104で復調された後、伝送時に発生された誤りがRSデコーディングを介して訂正され、ATVデコーダ110の伝送デマルチプレクサ105に入力されてデスクランプリングされる。

【0033】この際、マイクロコントローラ109はデスクランプリングされた制御信号及びデータを演算して、ス

マートカード103にデスクランプリングのための暗号化情報を伝送し、前記スマートカード103は伝送された暗号化情報を復号してATVデコーダ110に伝送する。この際、伝送デマルチプレクサ105がデスクランプリング情報に基づいて圧縮ビデオ信号、圧縮オーディオ信号、制御信号、及びデータを復元することになる。これにより、ビデオデコーダ107は圧縮オーディオ信号を伸張してメモリ106に一時貯蔵した後、その貯蔵データを出力して映像を表示し、オーディオデコーダ108は、圧縮オーディオ信号を伸張してオーディオを再生する。尚、マイクロコントローラ109は伝送デマルチプレクサ105から出力された制御信号及びデータを判読して、前記ビデオデコーダ107及びオーディオデコーダ108の動作を制御する。

【0034】一方、暗号化に使用されるいかなる方式の中で、DESのようなブロックサイバークリプター(Block-cipher)アルゴリズム及びPNシーケンスを用いたストリームサイバークリプター(Stream-cipher)アルゴリズムが一般的に一番広く使用されている。しかし、このような方式は暗号キー一つのみで暗号化及び復号化を行うので、キー管理(Key Management)及びキー分配(Key Distribution)が難しい。

【0035】従って、これに対する解決策として、U.S. Pat. No. 4200770のようなパブリックキー(Public-Key)暗号化方式が提案された。この方式は公開されたキーであるパブリックキーを用いて暗号化を行い、自身のみの秘密キー(Secret key)で復号を行うものである。そして、このようなパブリックキー暗号化方式を改善して暗号化システムで具現したのがU.S. Pat. No. 4405829であり、RSA暗号化アルゴリズムとして知られている。

【0036】

【発明が解決しようとする課題】しかし、前記パブリックキー暗号化方式は、高速暗号化には不適であるという短所がある。尚、CAシステムは不法複製を防止することを目的とするが、しかし、デジタルVCRのようなDSMを介して配布されるプログラムに対しては、不法複製に対して保護する方法がなかった。

【0037】即ち、DSMのような記録媒体によって供給されるプログラムに対する保護は、不法複製の防止を意味するが、既存のアナログVCRシステムに適用された複製防止(Copy Protection)方式は、デジタル方式の記憶媒体に適用し難く、且つ今までDSMのための複製防止方式に対する研究は別に進んでいない。

【0038】従って、本発明は、かかる問題点を解決するためのもので、その目的は、スクランプリングされたビットストリームとスクランプリングに使用された暗号化されたキーを互いに異なる経路で伝送して、暗号化されたキーをスマートカードで復号した後、その情報に基づいて、ビットストリームをデスクランプリングするように、ビットストリームのみでは正常的なデコードを行えない

ようにすることにより、不法視聴及び複写を防止するデジタル映像システムの不法視聴及び複写防止方法を提供することにある。

【0039】このような本発明は、C Aシステムでスマートカードを導入して自動的に料金をチェック(checking)する機能を含んでP P V(Pay Per View)機能を一層強力にし、スマートカードの代替により多様な機能を追加することで、システムの性能を簡単にアップグレード(Upgrade)させることができる。

【0040】尚、本発明は、伝送データを分離するので、保護するデータのキー分量を大幅減少させることができ、パワーオン時もしくは録画のためのデジタルV C R間の連結時に、自動的に認証及びキー交換過程を行うので、不法スマートカードでは動作されなくて、保護機能の信頼性をさらに向上させることになる。

【0041】

【課題を解決するための手段】本発明によるデジタル映像システムの不法視聴及び複写防止方法は、入力されるデータがスクランブル(scramble)されたかどうかを判別する判別段階と、前記判別段階でスクランブルされたデータと判別されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、キー情報に応じて前記分離されたビットストリームをデスクランブル(descramble)して、ディスプレイ装置にディスプレイする再生段階と、前記判別段階でスクランブルされたデータと判別されると、記録もしくは複写モードに応じてビットストリームとキーストリームが混合されたスクランブルされたデータ状態で記録媒体に記録したり、スクランブルされたデータをビットストリームとキーストリームに分離し、分離されたキーストリームを暗号化した後、ビットストリームと混合して記録媒体に記録する記録段階と、前記判別段階でスクランブルされたデータと判別されると、スクランブルされたデータをビットストリームとキーストリームに分離した後、「P C」モードもしくは「バックアップ・コピー(Back-up Copy)」モードに応じて分離されたキーストリームを記録側のキー情報に対して復号化して伝送したり、分離されたキーストリームを自身のキー情報と記録側のキー情報に対して2回暗号化して伝送する伝送段階とからなり、前記再生段階、記録段階、伝送段階は、同時又は選択的に行うことができ、そのことにより上記目的が達成される。

【0042】ある実施形態では、前記判別段階でスクランブルされていないデータと判別されると、スクランブルされていないデータは不法視聴及び複写防止機能を用いない。

【0043】ある実施形態では、前記再生段階は、分離されたキーストリームをM P E Gビットストリームに対応する復号化アルゴリズムで復号化して、キー情報を判読

する。ある実施形態では、前記記録段階の複写動作は、キーストリームを自身のキー情報に対して暗号化する第1段階と、第1段階で暗号化されたキーストリームが「P P C」モードであるか、或いは「バックアップ・コピー」モードであるかを判別する第2段階と、前記第2段階で「P P C」モードと判別されると、記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第3段階と、前記第2段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化し、その自身のキー情報に対して復号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第4段階と、からなっている。

【0044】ある実施形態では、前記第3段階の「P P C」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第1伝送段階と、前記第1伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、記録側のキー情報に対して復号化して伝送する第2伝送段階と、前記第2伝送段階で伝送されたキーストリームをインデックスコードに対応して記録側のキー情報に対して暗号化した後、前記第1伝送段階で伝送されたビットストリームに混合して記録媒体に記録する記録段階と、からなっているある実施形態では、前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム(S_{K5}(BS)+E₆(KS))をビットストリーム(S_{K5}(BS))とキーストリーム(E₆(KS))に分離した後、キーストリーム(E₆(KS))が分離された部分にインデックスコードI D Xを挿入する分離段階と、前記分離段階で分離されたキーストリーム(E₆(KS))を自身のキー情報に対して暗号化する暗号化段階と、前記暗号化段階で暗号化されたキーストリームを自身のキー情報とM P E Gビットストリームに対して復号化することによりキー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて前記分離されたビットストリーム(S_{K5}(BS))をデスクランブルする復号化段階と、を含んでいる。

【0045】ある実施形態では、前記第4段階の「バックアップ・コピー」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第1伝送段階と、前記第1伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、暗号化されたキーストリームを記録側のキー情報と自身のキー情報に対して復号化して伝送する第2伝送段階と、前記第2伝送段階で伝送されたキーストリームをインデックスコードに対応して、記録側のキー情報に対して暗号

化した後、前記第 1 伝送段階で伝送されたビットストリームに混合して、記録媒体に記録する記録段階と、からなっている。

【0046】ある実施形態では、前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)$)と $+dS_{AK}[E^6(KS)]$ を、ビットストリーム($S_{KS}(BS)$)とキーストリーム($dS_{AK}[E^6(KS)]$)を分離した後、キーストリーム($dS_{AK}[E^6(KS)]$)が分離された部分に、インデックスコード IDX を挿入する分離段階と、前記分離段階で分離されたキーストリームを自身のキー情報に対して 2 回暗号化されたキーストリームを自身のキー情報と MPEG ビットストリームに対して復号化することにより、キー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて、分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルする復号化段階と、を含んでいる。

【0047】本発明によるデジタル映像システムの不法視聴及び複写防止方法は、スクランブルされたデータが入力されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、判読されたキー情報に基づいて、前記分離されたビットストリームをデスクランブルして、ディスプレイ装置にディスプレイする再生段階と、スクランブルされたデータが入力されると、ビットストリームとキーストリームが混合されたスクランブルされたデータ状態で、記録媒体に記録する記録段階とからなり、前記再生段階、記録段階は、同時若しくは選択的に行うことができ、そのことにより上記目的が達成される。

【0048】ある実施形態では、前記再生段階は、分離されたキーストリームを、MPEG ビットストリームに対する復号化アルゴリズムで復号してキー情報を判読し、判読されたキー情報で、デスクランブル方式を判別する。

【0049】ある実施形態では、前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+E^6(KS)$)をビットストリーム($S_{KS}(BS)$)とキーストリーム($E^6(KS)$)に分離した後、キーストリーム($E^6(KS)$)が分離された部分に、インデックスコード IDX を挿入する分離段階と、前記分離段階で分離されたキーストリーム($E^6(KS)$)を自身のキー情報に対して、暗号化アルゴリズムで暗号化する暗号化段階と、前記暗号化段階で 2 回暗号化されたキーストリームを、自身のキー情報と MPEG ビットストリームに対して復号化することにより、キー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて、前記分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルして、ディスプレイ装置にディスプレイする復号化段階と、を含んでいる。

【0050】本発明によるデジタル映像システムの不法視聴及び複写防止方法は、複写時に自身のキー情報に対して暗号化されたキーストリームが伝送されると、「バックアップ・コピー」モードであるか、もしくは「PPC」モードであるかを判別する判別段階と、前記判別段階で「PPC」モードと判別されると、記録側のキー情報に対して前記キーストリームを復号して伝送する第 1 伝送段階と、前記第 1 伝送段階で伝送されたキーストリームを記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入して、ビットストリームのように記録媒体に記録する第 1 記録段階と、前記判別段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して、キーストリームを 2 回復号化して伝送する第 2 伝送段階と、前記第 2 伝送段階で伝送されたキーストリームを、記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入してビットストリームのように記録媒体に記録する第 2 記録段階と、からなっており、そのことにより上記目的が達成される。

【0051】ある実施形態では、前記第 1 伝送段階は、自身のキー情報 Ak に対して暗号化されたキーストリームを自身のキー情報 Ak に対して復号化し、さらに記録側のキー情報 A1 に対して復号化した後、伝送する。

【0052】ある実施形態では、前記第 2 伝送段階は、自身のキー情報 Ak に対して暗号化されたキーストリームを、自身のキー情報 Ak に対して 2 回復号化し、さらに記録側のキー情報 A1 に対して復号化した後伝送する。

【0053】本発明によるデジタル映像システムの不法視聴及び複写防止方法は、記録媒体の再生時にキーストリーム($E^6(KS)$)が検出されると「PPC」記録媒体と判別して、キーストリームを自身のキー情報に対して暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いて、ビットストリームをデスクランブルする「PPC」モード再生段階と、記録媒体の再生時に自身のキー情報に対して復号化されたキーストリーム($dS_{AK}[E^6(KS)]$)が検出されると、「バックアップ・コピー」記録媒体と判別して、自身と記録側のキー情報に対して 2 回暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いてビットストリームをデスクランブルする「バックアップ・コピー」モード再生段階と、からなっており、そのことにより上記目的が達成される。

【0054】本発明によるデジタル映像システムの不法視聴及び複写防止装置は、アナログ放送信号を変復調して RS デコードする復調及び誤り訂正手段と、前記復調及び誤り訂正手段の出力を記録/再生装置に伝送し、

その記録／再生装置で再生されるスクランブルされた記録信号をビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する複写防止処理手段と、前記復調及び誤り訂正手段若しくは複写防止処理手段から出力されるビットストリームをデスクランプリング情報に基づいてデスクランブルするデコーダ手段と、前記複写防止処理手段で暗号化されたキーストリームを復号して、前記デコーダ手段へデスクランプリング情報として出力するスマート手段と、から構成しており、そのことにより上記目的が達成される。

【0055】ある実施形態では、前記復調及び誤り訂正手段が接続されたデコーダ手段をスマート手段に接続して、前記スマートカードで前記デコーダ手段のキーストリームを自身のキー情報で復号して、デスクランプリング情報を前記デコーダ手段へ出力することにより、不法視聴防止機能を行うように構成されている。

【0056】ある実施形態では、前記復調及び誤り訂正手段が接続された複写防止処理手段が、デジタル記録／再生装置に接続されて初めに録画を行う。

【0057】ある実施形態では、前記デジタル記録／再生装置が接続された複写防止手段のキーストリームラインをスマートカードに接続するとともにビットストリームラインをデコーダ手段に接続し、前記複写防止処理手段とデコーダ手段を接続して、前記スマートカードが前記デコーダ手段のインデックスコードに対応する前記複写防止処理手段のキーストリームを自身のキー情報で復号して、前記デコーダ手段へ出力することにより、不法再生を防止する。

【0058】ある実施形態では、前記複写防止処理手段は「PPC」モードの記録媒体再生時にデジタル記録／再生装置の再生データから分離したキーストリームを自身のキー情報で暗号化して、スマートカードへ伝送する。

【0059】ある実施形態では、前記複写防止処理手段は、「バックアップ・コピー」モードの再生媒体再生時にデジタル記録／再生装置の再生データから分離したキーストリームを、自身のキー情報で2回暗号化してスマートカードへ伝送する。

【0060】ある実施形態では、前記複写防止処理手段は、スマートカード固有のキー情報を記憶するRAMと、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、前記RAMのキー情報で前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサと、からなっている。

【0061】ある実施形態では、前記スマートカードは、ビットストリームのための復号化アルゴリズムプログラムを貯蔵する第1アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第2アルゴリズム貯蔵メモリと、自身のキー情報を貯蔵するROMと、他のスマートカードのキー情報を一時的に貯蔵するRAM

と、から構成している。

【0062】本発明によるデジタル映像システムの不合法視聴及び複写防止装置は、第1デジタル記録／再生装置の再生データをビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する第1複写防止処理手段と、前記第1複写防止処理手段で暗号化されたキーストリームを自身のキー情報と記録側のキー情報に対して復号化する第1、第2スマートカードと、前記第2スマートカードを介して伝送された前記第1スマートカードのキーストリームを自身のキー情報で暗号化した後、暗号化されたキーストリームを分離されたビットストリームとともに、第2デジタル記録／再生装置へ出力して、記録媒体に記録する第2複写防止処理手段と、から構成しており、そのことにより上記目的が達成される。

【0063】ある実施形態では、前記第1複写防止処理手段は、キーストリームを自身のキー情報Akに対して暗号化した後、第1スマートカードへ伝送する。

【0064】ある実施形態では、前記第1スマートカードは、「PPC」モードである時、第1複写防止処理手段のキーストリームを自身のキー情報と記録側のキー情報に対して復号化した後、第2スマートカードへ伝送する。

【0065】ある実施形態では、前記第2複写防止処理手段は、第2スマートカードで伝送されるキーストリームを、自身のキー情報Aiに対して暗号化した後、第1複写防止処理手段のビットストリームと混合する。

【0066】ある実施形態では、前記第1スマートカードは「バックアップ・コピー」モードであるとき、第1複写防止処理手段のキーストリームを、自身のキー情報に対して2回復号した後、記録側のキー情報に対して復号する。

【0067】ある実施形態では、前記第2複写防止処理手段は、第2スマートカードから伝送されるキーストリームを自身のキー情報に対して暗号化し、その暗号化されたキーストリームをビットストリームと混合する。

【0068】ある実施形態では、前記第1、第2複写防止処理手段は、スマートカード固有のキー情報を貯蔵するRAMと、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、前記RAMのキー情報によって、前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサと、から構成している。

【0069】ある実施形態では、前記第1、第2スマートカードは、ビットストリームのための復号化アルゴリズムプログラムを貯蔵する第1アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第2アルゴリズム貯蔵メモリと、自身のキー情報を貯蔵するROMと、他のスマートキー情報を一時的に貯蔵するRAMと、から構成している。

【0070】

【発明の実施の形態】以下、本発明を添付図面を参照して詳細に説明する。

【0071】本発明はデジタル信号を記録及び再生し得る全ての記録/再生装置に適用可能であり、本発明では説明の便宜のためにDVCＲを一実施例としている。

【0072】従って、本発明の実施例は図7に示すように、アナログの放送信号を変復調してRSデコードする復調及び誤り訂正部1と、デスクランプリング情報に基づいて前記復調及び誤り訂正部1の出力をデスクランブルするATVデコーダ2と、スクランブルされた記録信号をビットストリームとキーストリームに分離し、分離されたキーストリームを暗号化する複写防止処理部4と、この複写防止処理部4で分離されて暗号化されたキーストリーム及び前記ATVデコーダ2のインデックスコードを復号して前記ATVデコーダ2にデスクランプリング情報Kを出力するスマートカード3とから構成する。

【0073】前記複写防止処理部4は図8に示すように、スマートカード固有のキー情報を貯蔵するRAM17と、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵部18と、前記RAM17のキー情報で前記アルゴリズム貯蔵部18の暗号化プログラムを実行するプロセッサ16とから構成する。

【0074】前記スマートカード3は図9に示すように、ビットストリームのための復号化アルゴリズムを貯蔵する第1アルゴリズム貯蔵部12と、自身の復号化アルゴリズムを貯蔵する第2アルゴリズム貯蔵部13と、自身のキー情報を貯蔵するROM14と、他のスマートカードのキー情報を一時貯蔵するRAM15と、前記ROM14若しくはRAM15に貯蔵されたキー情報に対して前記第1、第2アルゴリズム貯蔵部12、13の貯蔵アルゴリズムで暗号化若しくは復号化を実行するプロセッサ11とから構成する。

【0075】この際、前記プロセッサ11、16はワイヤロジック(Wired Logic)で構成するか、或いはマイクロプロセッサを用いることができ、マイクロプロセッサを用いる場合、スマートカードのための暗号化アルゴリズムはプログラムで内蔵することになる。

【0076】以下、このように構成した本発明の動作及び作用効果を説明する。

【0077】本発明でMPEGビットストリームが図11(a)乃至(c)のようなフォーマットで伝送されるが、図11(a)はスクランブルされていないフォーマットであり、図11(b)はビットストリームに対してスクランブルされたフォーマットであり、図11(c)はビットストリームが選択的にスクランブルされたフォーマットである。

【0078】本発明ではMPEGビットストリームに対してスクランブルされた場合、どんな形態でも保護(protection)が加わると前提する。

【0079】従って、複写防止処理部4に図11(b)若しくは(c)のようなフォーマットのスクランブルされたストリームデータ($S(KS(BS)+E(KS))$)が入力された場合、図10に示すようにスプリッタ(Splitter)で図11(d)乃至(e)のようなビットストリーム($S(KS(BS)+I(KS))$)とキーストリーム($E(KS)$)に分離し、記録モードを行うと、前記分離されたキーストリーム($E(KS)$)はさらに暗号化されてスマートカード3へ伝送される。

【0080】ここで、図11(c)に示すように、ビットストリームが部分的にスクランブルされた場合には、スクランブルされた部分に対してのみ不法視聴及び複写防止機能を適用するので、部分的な保護機能を行うことができる。

【0081】まず、図11(a)に示すように、スクランブルされていないビットストリームが伝送された場合、復調及び誤り訂正部1で変復調及び復号されたビットストリームが複写防止処理部4に入力されてもスマートカード3へデータを伝送せず、前記復調及び誤り訂正部1のビットストリームが入力されたATVデコーダ2も前記スマートカード3にデータを伝送することなくビットストリームを復号する。従って、視聴及び複写に何の制限もなくする。

【0082】ここで、チューナから復調及び誤り訂正部1に入力される信号とATVデコーダ2から出力されるビデオ及びオーディオ信号はアナログ信号である。チューナから出力される信号は、GAビットストリームからのVSB変調された信号である。そして、入出力信号のうち、ビットストリームとキーストリームはデジタルDVCＲのためのデジタル信号である。この際、記録を行うと、デジタルVCRにビットストリームが記録され、この記録されたビットストリームは一般的なデジタルVCRで再生される。つまり、スクランプリングがわからないMPEGビットストリームが複写防止処理部4に入力されて、図10に示すようにスプリッタを通過してもキー情報が無いためにスマートカード3へ伝送されるデータが無いので、スクランプリングがわからない場合には、視聴及び複写に何の制限もない。

【0083】尚、本発明は、録画若しくは複写防止機能を行う場合、ビットストリームとキーストリームに分離され、それぞれ異なるラインで伝送されるが、複写防止方法に関する情報はPESヘッダ内の付加複写情報(Additional Copy Info.)フィールドに載せられて伝送される。

【0084】この際、暗号化されたキーがないスクランブルされたビットストリームを、パブリックチャンネルで伝送しても、キーに関する情報が除去された状態なので、不法使用者に流出した場合には、確にデスクランプリングを行うことができない。そして、分離されたキーはさらに暗号化されて伝送されるので、復号アルゴリズムがない場合には、ビットストリームをデスクランブル

することができない。従って、本発明はかかる不法視聴及び複写防止のために MPEG 伝送プロトコルで任意のフィールドを用いるが、スクランブルされたビットストリームは、複写防止機能が適用されたものである。

【0085】まず、「Transport-scrambling-control フィールド」を「Not Scrambled」モードに変えておけば、デコーダ 2 では、デスクランプリングを行わないので、不法使用者は前記フィールドを操作することができない。このような複写防止方法は、「Transport-scrambling-control フィールド」によって複写防止されるようにするか、或いは複写可能(free-copy)となるようにするかを決定するので、不法使用者はこのフィールドを操作することだけでは、複写防止機能を解除することができない。

【0086】次に、不法使用者が PES ヘッダ内の「付加複写情報(Additional Copy Info.)フィールド」を修正する方法で、このフィールドの修正是保護方法を変換させるものであって、保護方法自体を解体するものではないので、複写防止機能に大きな損傷を与えない。

【0087】このような特徴を有する本発明によって支握される複写防止方法は、CA 機能である PPV (Pay Per View)、PPP (Pay Per Play) 機能をデフォルト(Default)とし、「No Copy」方法、「PPC (Pay Per Copy)」方法、「Back-up Copy」方法がある。

【0088】ここで、「No Copy」方法は、他のビデオテープで複写を全くできないようにする方法であり、「PPC」方法は、1 回複写ごとに料金を受けるものであり、「Back-up Copy」方法は、一側のデジタル VCR で再生されるビデオテープを他側のデジタル VCR で複写した時に複写されたビデオテープは一側のデジタル VCR でのみ正常的に表示可能であり、他側のデジタル VCR では表示し得ない方法である。

【0089】以下、本発明の複写防止方法及びそれによる MPEG ビットストリームの流れを図 19 乃至図 22 を参照して説明する。

【0090】図 19 および 20 は、記録若しくは再生モード時に複写防止処理部の動作に対する信号流れ図であり、図 21 は前記複写防止処理部に対応するスマートカードの動作に対する信号流れ図であり、図 22 は記録若しくは再生動作時のキー交換及び認証過程に対する信号流れ図である。

【0091】まず、図 19 の信号流れを説明する。ビットストリームが入力された複写防止処理部 4 は、キー情報の有無を確認してスクランプリングの如何を判別し、キー情報があつてスクランブルされた場合、最初の録画であるか或いは複写録画であるかを判別する (S101)。

【0092】即ち、スクランブルされたデータの場合、ビットストリーム(S_{KS}(BS))とキーストリーム(E_K(KS))の分離により S_{KS}(BS)+DX 形態のストリームで伝送されるかどうかを検索して、S_{KS}(BS)+DX 形態のストリー

ムが検出されると複写録画と判別し、検出されなければ最初の録画と判別する (S102)。

【0093】これにより、最初録画と判別された場合、VCR5 でビットストリームとキーストリーム(S_{KS}(BS)+DX)をテープに録画し (S106)、複写録画と判別された場合、キーストリーム(E_K(KS))が分離されたビットストリーム(S_{KS}(BS)+DX)を記録側の複写防止処理部 8 に伝送するとともに、前記キーストリーム(E_K(KS))をキー情報 A k に対して、さらに暗号化した後 (S105)、その暗号化されたキーストリーム(E_{SK}^{Ak}[E_K(KS)])をスマートカード 3 を介して、記録側のスマートカード 7 に伝送することにより、記録側の VCR9 でテープに録画することになる (S106)。

【0094】逆に、図 20 は、図 19 のような信号流れで録画をしたテープを再生する場合の信号流れ図である。複写防止処理部 4 は、VCR で再生されたビットストリームが入力されると (S107)、キーストリームを分離して判別することにより (S108)、録画機能が「Back-up Copy」であるかどうかを判別することになる (S110)。

【0095】この際、前記段階 (S110) はキー情報がないければ、一般的な録画テープと判別し、暗号化されたキーストリーム(E_K(KS))が検出されると最初録画テープと判別する。尚、自身のキー情報 A k に対して復号されたキーストリーム(D_{SK}^{Ak}[E_K(KS)])が検出されると、PPC 機能の録画テープと判別し、他のスマートカードのキー情報 A i に対して復号されたキーストリーム(D_{SK}^{Ai}[E_K(KS)])が検出されると、「Back-up Copy」機能の録画テープと判別する。これにより、複写防止処理部 4 は、一般録がテープの場合には、ビットストリーム(BS)を、複写防止用録画テープの場合には、キーストリーム(E_K(KS))が分離されたビットストリーム(S_{KS}(BS)+DX)をデコーダ 2 に伝送する (S109)。

【0096】そして、複写防止処理部 4 は複写防止用録画テープの再生時に Back-up Copy 機能が適用された場合、キーストリーム(D_{SK}^{Ak}[E_K(KS)])を自身のキー情報 A k に対して暗号化アルゴリズム E_{SK}^{Ak}(・) で 2 回暗号化することにより、暗号化されたキーストリーム(E_{SK}^{Ak}[E_K(KS)])をスマートカード 3 に伝送し (S111、S112、S113)、Back-up Copy 機能が適用されていない場合、キーストリーム(E_K(KS))を自身のキー情報 A k に対して暗号化アルゴリズム E_{SK}^{Ak}(・) で暗号化することにより、暗号化されたキーストリーム(E_{SK}^{Ak}[E_K(KS)])をスマートカード 3 に伝送する (S112、S113)。

【0097】前記のような動作を複写防止処理部 4 で行うとき、スマートカード 3 は図 21 のような信号流れの動作を行う。これを詳しく説明すると、前記スマートカード 3 は放送若しくは再生を行うことにより、デコーダ

2でインデックスコードID_X若しくはキーストリーム(E^G(KS))が入力されるかどうかを判別する(S114、S115)。

【0098】この際、インデックスコードID_Xではないキーストリーム(E^G(KS))が入力されると、PPV機能の放送視聴と判別したスマートカード3は、前記キーストリーム(E^G(KS))をビットストリームGAに対する復号化アルゴリズムD_G(・)で復号して(S116)、キー情報KSをデコーダ2に入力させる(S117)。これにより、デコーダ2はスマートカード3のキー情報KSを判読してデスクランプリング方式を判別し、その判別されたデスクランプリング方式でビットストリーム(S_{K5}(BS))をデスクランブルしてアナログビデオ信号及びオーディオ信号として出力することにより、視聴者は放送を視聴することができる。

【0099】一方、前記段階(S115)でインデックスコードID_Xが入力されると判別されると、スマートカード3は複写防止処理部4で入力されたキーストリーム(E^S_{Ak}[E^G(KS)])をキー情報Akに対して復号化アルゴリズム(D^S_{Ak}(・))で復号した後(S118)、再生動作が若しくは記録動作かを判別する(S119)。

【0100】この際、前記段階(S119)で再生動作と判別されると、スマートカード3は復号化されたキーストリーム(E^G(KS))をビットストリームGAに対する復号化アルゴリズム(D_G(・))で復号して(S116)、キー情報KSをデコーダ2に入力させる(S117)。これにより、デコーダ2はスマートカード3のキー情報KSを判読して、デスクランプリング方式を判別し、その判別されたデスクランプリング方式で複写防止処理部4で分離されたビットストリーム(S_{K5}(BS))をデスクランブルして、アナログビデオ信号及びオーディオ信号を出力することにより、視聴者はテープの録画プログラムを視聴することができる。

【0101】そして、前記段階(S119)で記録動作と判別されると、スマートカード3は「Back-up Copy」機能であるかどうかを判別する(S120)。「Back-up Copy」機能であれば、キーストリーム(E^G(KS))をキー情報Akに対して、復号化アルゴリズム(D^S_{Ak}(・))で復号して(S121)、復号化されたキーストリーム(D^S_{Ak}[E^G(KS)])をキー情報A1に対して、復号化アルゴリズム(D^S_{Ak}(・))で復号化することになる(S122)。

【0102】この際、スマートカード3で復号化されたキーストリーム(D^S_{A1}[D^S_{Ak}[E^G(KS)]))が記録側に伝送され(S123)、スマートカード7を介して複写防止処理部8に入力されると(S124)、暗号化アルゴリズム(E^S_{A1}(・))で暗号化される。これにより、スマートカード7は暗号化されたキーストリーム(D^S_{Ak}[E^G(KS)])をインデックスコードID_Xが指定する位置に混入させて再生側の複写防止処理部4から出力されたビット

ストリーム(S_{K5}(BS))と混合すると、VCR9でテープに録画することになる。

【0103】一方、前記段階(S119)で記録動作と判別され、且つ前記段階(S120)で「Back-up Copy」機能ではないPPC機能が適用されたと判別されると、スマートカード3は、キーストリーム(E^G(KS))をキー情報A1に対して復号化アルゴリズム(D^S_{A1}(・))で復号化し(S122)、その復号化されたキーストリーム(D^S_{A1}[E^G(KS)])を記録側へ伝送することになる(S123)。

【0104】この際、スマートカード7を介してキーストリーム(D^S_{A1}[E^G(KS)])の入力を受けた記録側の複写防止処理部8は、暗号化アルゴリズム(E^S_{A1}(・))で暗号化した後、その暗号化されたキーストリーム(E^G(KS))をインデックスコードID_Xが指定する位置に混入させて、再生側の複写防止処理部4から出力されたビットストリーム(S_{K5}(BS))と混合することになる。

【0105】従って、複写防止処理部8から出力されたビットストリーム(S_{K5}(BS)+E^G(KS))はVCR9によってテープに録画される。

【0106】上述したように、本発明では全てのスマートカードがMPEGビットストリームに対する暗号化アルゴリズム(E^G(・))と復号化アルゴリズム(D_G(・))に対して共通のアルゴリズム及び共通のキーを持つ。

【0107】そして、スマートカードに対する暗号化アルゴリズム(E^S_{A1}(・))と復号化アルゴリズム(D_S_{Ak}(・))は全てのスマートカードが共通のアルゴリズムを持つが、キー情報はスマートカードによって異なる。即ち、各スマートカードは自身の認識番号IDに該当する認証キーを内蔵することになる。

【0108】前記のような動作を行うに当たり、複写防止処理部とスマートカード間、スマートカードとスマートカード間に相手方を認識し得る認証過程及びキーを交換する過程を含む処理動作が必要である。この際、認証過程はDESアルゴリズムのような対称キーアルゴリズムを用いる方法や、RSAのようなパブリックキーアルゴリズムを用いる方法や、FS(Fiat-Shamir)Schemeを用いる方法等の多様な方法が提示されている。

【0109】本発明では、パブリックキーアルゴリズムを用いる認証過程を行うとともに、キーを交換する方法の例を図22に示したが、このような方法はパブリックキー(n、e)を認証しよとするキー受信手段201とキー伝送手段202が共有しているという前提のもとで、適用することになる。

【0110】この際、キー受信手段201は複写防止処理部若しくは記録側のスマートカード7であり、キー伝送手段202は自身のスマートカードkである。

【0111】以下、前記のような流れで動作する本発明の実施例を図12乃至図18を参照して説明する。

【0112】本発明では図11(a)のようなスクラン

ブルされていないビットストリームB Sが伝送された場合、図12に示すように回路が動作するので、復調及び誤り訂正部1で復調及びR Sデコードされたビットストリームがデコーダ2で復号されるにより、アナログビデオ及びオーディオ信号が出力される。

【0113】この際、記録の場合、復調及び誤り訂正部1から出力されるビットストリームB Sは、複写防止処理部4を介してVCR5でテープに記録され、再生の場合、VCR5で再生されたビットストリームB Sが複写防止処理部4を介してデコーダ2に入力されて復号されることによりアナログビデオ及びオーディオ信号が出力される。即ち、複写防止処理部4からスマートカード3へデータを出力しないので、視聴及び複写に影響を与えない。

【0114】そして、図11 (c) 又は (c) のようなスクランブルされたビットストリームが入ってくる場合、CA機能を適用することにより、図13において図18のような動作を行う。

【0115】まず、PPV機能を行う場合、図13のような信号流れで動作するが、スクランブルされたビットストリーム(S_{K5}(B_S))と暗号化されたキーストリーム(E⁶(K_S))が伝送されると、復調及び誤り訂正部1は復調された入力信号を復調した後、R Sデコーディングを介して伝送中に発生した誤りを訂正することになる。

【0116】この際、デコーダ2が復調及び誤り訂正部1の出力(S_{K5}(B_S)+E⁶(K_S))のうち、キーストリーム(E⁶(K_S))を分離してスマートカード3へ出力すると、スマートカード3は前記暗号化されたキーストリーム(E⁶(K_S))を復号してキーストリームK Sを前記デコーダ2にさらに出力する。これにより、デコーダ2はスマートカード3のキーストリームK Sを判読してデスクランプリング方式を判別した後、ビットストリーム(S_{K5}(B_S))を復号してアナログビデオ信号及びオーディオ信号を出力することになる。

【0117】ここで、図9のようなスマートカード3はプロセッサ11が復号化アルゴリズム(E⁶(・))で暗号化されたキーストリーム(E⁶(K_S))を復号して、その復号されたキーストリームK Sをデコーダ2へ出力することになる。

【0118】一方、スクランブルされたビットストリームを最初に録画する場合、図14のような信号流れで動作するが、伝送されたビットストリーム(S_{K5}(B_S)+E⁶(K_S))は、復調及び誤り訂正部1で復調及びR Sデコーディングを介して誤りが訂正された後、複写防止処理部4を介してVCR5に入力されてテープに録画される。

【0119】このように録画されたビットストリームを再生する場合、PPP機能であるとき、図15のような信号流れで動作するが、VCR5で再生されたビットストリーム(S_{K5}(B_S)+E⁶(K_S))が複写防止処理部4に入力されると、複写防止処理部4は再生されたビットストリ

ーム(S_{K5}(B_S)+E⁶(K_S))をビットストリーム(S_{K5}(B_S))とキーストリーム(E⁶(K_S))に分離した後、前記分離されたキーストリーム(E⁶(K_S))を暗号化アルゴリズム(E⁵C_{Ak}(・))でさらに暗号化して、スマートカード3へ出力し、前記分離されたビットストリーム(S_{K5}(B_S))はキーストリーム(E⁶(K_S))が取り出された部分にインデックスコードID Xを付加してデコーダ2へ出力する。

【0120】この際、デコーダ2を介してインデックスコードID Xの入力を受けたスマートカード3は、複写防止処理部2の暗号化されたキーストリーム(E⁵C_{Ak}[E⁶(K_S)])をスマートカードのための復号化アルゴリズム(D⁵C_{Ak}(・))で復号して、デスクランプリング情報であるキーストリームK Sを前記デコーダ2へ出力する(S117)。これにより、デコーダ2はスマートカード3のキーストリームK Sを判読してデスクランプリング方式を判別した後、複写防止処理部4を介して入力されたビットストリーム(S_{K5}(B_S))を復号することにより、アナログビデオ信号及びオーディオ信号を出力することになる。

【0121】そして、図14のような信号流れで録画されたデータを異なるVCRで録画する場合、図16の信号流れのようにPPV機能を行うが、VCR5で再生されたビットストリーム(S_{K5}(B_S)+E⁶(K_S))が複写防止処理部4に入力されると、複写防止処理部4は、ビットストリーム(S_{K5}(B_S)+E⁶(K_S))を、ビットストリーム(S_{K5}(B_S))と、キーストリーム(E⁶(K_S))とに分離する。その後、前記分離されたキーストリームを暗号化アルゴリズム(E⁵C_{Ak}(・))でさらに暗号化してスマートカード3へ出力し、前記分離されたビットストリーム(S_{K5}(B_S))とキーストリーム(E⁶(K_S))が取り出された部分にインデックスコードID Xを付加して記録側の複写防止処理部8へ出力することになる。

【0122】この際、再生側のスマートカード3は、複写防止処理部4で暗号化されたキーストリーム(E⁵C_{Ak}[E⁶(K_S)])をRAMに貯蔵されたキー情報A1に対して復号化アルゴリズム(D⁵C_{A1}(・))で復号した後、その復号されたキーストリーム(D⁵C_{A1}[E⁶(K_S)])を記録側のスマートカード7へ出力することになる。これにより、記録側のスマートカード7が再生側のスマートカード3のキーストリーム(D⁵C_{A1}[E⁶(K_S)])の入力を受けて記録側の複写防止処理部8へ出力すると、前記複写防止処理部8は前記キーストリーム(D⁵C_{A1}[E⁶(K_S)))を暗号化して元の暗号化されたキーストリーム(E⁶(K_S))に復元した後、インデックスコードID Xによって再生側の複写防止処理部4から出力されたビットストリーム(S_{K5}(B_S))に混合してVCR5へ出力することにより、他のテープに録画することになる。

【0123】このような動作で録画されたテープのデータはPPP機能を通して、図15のような信号流れで再生することができる。尚、図14のような信号流れで

録画されたデータを他のVCRで録画する場合、図17の信号流のようにBack-upCopy機能を行うことができる。

【0124】つまり、VCR5で再生されたビットストリーム $(S_{KS}(BS)+E_6(KS))$ が複写防止処理部4に入力されると、複写防止処理部4はビットストリーム $(S_{KS}(BS))$ とキーストリーム $(E_6(KS))$ に分離した後、前記分離されたキーストリームを暗号化アルゴリズム $(E_{SAK}(\cdot))$ でさらに暗号化してスマートカード3へ出力し、前記分離されたビットストリーム $(S_{KS}(BS))$ はキーストリーム $(E_6(KS))$ が取り出された部分にインデックスコードIDXを付加して記録側の複写防止処理部8へ出力することになる。

【0125】この際、再生側のスマートカード3は複写防止処理部4で暗号化されたキーストリーム $(E_{SAK}[E_6(KS)])$ をROMに貯蔵された自身のキーA_kに対して復号化アルゴリズム $(D_{SAK}(\cdot))$ で2回復号化した後、さらにRAMに貯蔵されたキー情報A₁に対して復号化アルゴリズム $(D_{SA1}(\cdot))$ で復号して、その復号されたキーストリーム $(D_{SA1}[D_{SAK}[E_6(KS)]])$ を記録側のスマートカード7に出力することになる。これにより、再生側のスマートカード3のキーストリーム $(D_{SA1}[D_{SAK}[E_6(KS)]])$ が記録側のスマートカード7を介して記録側の複写防止処理部8へ出力されると、複写防止処理部8は前記キーストリーム $(D_{SA1}[D_{SAK}[E_6(KS)]])$ をキー情報A₁に対して暗号化することにより、元の暗号化キーストリーム $(D_{SAK}[E_6(KS)])$ に復元する。そして、復元された暗号化キーストリーム $(D_{SAK}[E_6(KS)])$ を、インデックスコードID_Xによって再生側の複写防止処理部4から出力されたビットストリーム $(G_{KS}(BS))$ に混合して、VCR9へ出力して、他のテープに録画することになる。

【0126】ここで、料金は改善されたスマートカード3若しくは7で計数する。

【0127】このようなBack-up Copy機能を行って録画されたデータは元テープを録画したVCRでのみ再生することができるが、正常な再生の場合、図18(a)のような信号流で動作を行う。

【0128】つまり、VCR5で再生されたビットストリーム $(S_{KS}(BS)+E_{SAK}[E_6(KS)])$ が複写防止処理部4に入力されると、複写防止処理部4は、ビットストリーム $(S_{KS}(BS))$ とキーストリーム $(D_{SAK}[E_6(KS)])$ に分離する。その後、前記分離されたキーストリーム $(D_{SAK}[E_6(KS)])$ を暗号化アルゴリズム $(E_{SAK}(\cdot))$ で2回暗号化して、スマートカード3へ出力し、前記分離されたビットストリーム $(S_{KS}(BS))$ は、キーストリーム $(D_{SAK}[E_6(KS)])$ が取り出された部分に、インデックスコードID_Xを付加してデコーダ2へ出力する。

【0129】この際、デコーダ2を介してインデックスコードID_Xの入力を受けたスマートコード3は複写防

止処理部2で暗号化されたキーストリーム $(E_{SAK}[E_6(KS)])$ をスマートカードのための復号化アルゴリズム $(D_{SAK}(\cdot))$ で復号して、デスクランプリング情報であるキーストリームKSを前記デコーダ2へ出力する。これにより、デコーダ2はスマートカード3のキーストリームKSを判別してデスクランプリング方式を判別した後、複写防止処理部4を介して入力されたビットストリーム $(S_{KS}(BS))$ を復号することにより、アナログビデオ信号及びオーディオ信号を出力することになる。

【0130】そして、最初録画されたVCRではない他のVCRで再生する非正常再生の場合、図18(b)のような信号流で動作することになって、テープの再生が不可能となる。

【0131】つまり、テープ複写を行ったVCR9で複写テープを再生すると、複写防止処理部8では再生されたデータ $(S_{KS}(BS)+E_{SAK}[E_6(KS)])$ をスプリッティング処理して、ビットストリーム $(S_{KS}(BS)+ID_X)$ を分離する。

【0132】この際、分離されたキーストリーム $(D_{SAK}[E_6(KS)])$ は自身のキー情報A₁に対して暗号化された後、さらにキー情報A₁に対して暗号化 $(E_{SA1}[E_{SAK}[D_{SAK}[E_6(KS)]])$ されてスマートカード7へ伝送される。そして、スマートカード7はビットストリーム $(E_{SA1}[E_{SA1}[D_{SAK}[E_6(KS)]])$ を復号できないので、デコーダ6にキー情報KSを伝送しない。これにより、スマートカード7はビットストリーム $(S_{KS}(BS))$ をデスクランブルしないので、複写テープの再生が行われない。

【0133】一方、本発明の理解のために、本発明に使用された用語を定義すると、下記の通りである。

【0134】1) BS: スクランブルされていないGAビットストリーム

2) KS = $[K_0, K_1, K_2, \dots, K_i, \dots, K_n]$: キーストリーム

ここで、nはスクランプリングに使用されたキーの総数
3) BS = $[BS_0, BS_1, BS_2, \dots, BS_i, \dots, BS_n]$: ビットストリーム

ここで、BS_iはBSの一つのセグメントとして、スクランブルする単位

4) S_{K5}(BS): スクランブルされたMPEGビットストリーム

$S_{KS}(BS) = [SK_0(BS_0), SK_1(BS_1), \dots, SK_i(BS_i), \dots, SK_n(BS_n)]$

5) E(·) & D(·): GAでキーを暗号化及び復号化するに使用されたアルゴリズム

$E_6(KS) = [E_6(K_0), E_6(K_1), \dots, E_6(K_i), \dots, E_6(K_n)]$
 $D_6(KS) = [D_6(K_0), D_6(K_1), \dots, D_6(K_i), \dots, D_6(K_n)] = KS$

6) ID_X: $[0, 1, 2, \dots, i, \dots, n]$: i

ンデックスストリーム7) A k : スマートカード (k) の認証キー

8) $E^{SC_A}(\cdot)$ & $D^{SC_A}(\cdot)$: スマートカードの認証キー (A) をキーとしたスマートカードの暗号化及び復号化アルゴリズム。

【0135】

【発明の効果】 以上説明したように、本発明はパワーオン時若しくはデジタルVCR間の連結時に、自動的に認証及びキー交換過程を行うので、不法スマートカードに対する不法視聴及び複写防止機能を自動的に行うことが出来、さらに部分的に不法視聴及び複写防止を行うことができるので、プログラムの保護を願う部分にスクランプリング処理を行うと、自動的に不法視聴及び複写防止を行いながら料金も所望通りに賦課することができる。

【0136】 そして、本発明はビットストリームと分離させたキーストリームを異なる経路で伝送するので、保護データの量を減少させることができ、且つスマートカードに不法視聴防止と不法複写防止機能を見現するとき、PPV、PPP、PPC及びBack-up Copy機能を区別するようにすることで、各機能に対して差別的に料金を賦課することができる。

【0137】 尚、本発明はDSM应用到適用し得るデジタル信号の複写防止機能を見現することにより、デジタルVCRのようなDSMにおけるプログラム著作権保護に適用することができる。従って、本発明を適用すると、不法視聴及び複写防止に対する信頼性を向上させることができるという効果が得られる。

【図面の簡単な説明】

【図1】 一般的なスクランブラのブロック図である。

【図2】 一般的なデスクランブラのブロック図である。

【図3】 伝送フォーマットの例示図である。

【図4】 図3におけるPESヘッダの詳細例示図である。

【図5】 キー分配による伝送フォーマットの例示図である。

【図6】 従来のATVデコーダのブロック図である。

【図7】 本発明の不法視聴及び複写防止装置のブロック図である。

【図8】 図7における複写防止処理部の詳細ブロック図である。

【図9】 図7におけるスマートカードの詳細ブロック図である。

【図10】 図8におけるビットストリームのスプリッティング(splitting)を示す例示図である。

【図11】 (a)~(f)は、各ビットストリームのフォーマットを示す例示図である。

【図12】 本発明の接続状態を示す例示図である。

【図13】 本発明の接続状態を示す例示図である。

【図14】 本発明の接続状態を示す例示図である。

【図15】 本発明の接続状態を示す例示図である。

【図16】 本発明の接続状態を示す例示図である。

【図17】 本発明の接続状態を示す例示図である。

【図18】 本発明の接続状態を示す例示図である。

【図19】 本発明の動作のための信号流れ図である。

【図20】 本発明の動作のための信号流れ図である。

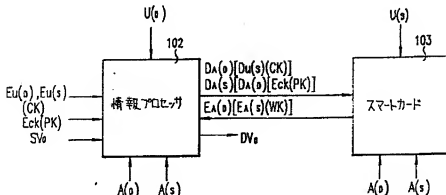
【図21】 本発明の動作のための信号流れ図である。

【図22】 本発明によるキー交換及び認証過程のための信号流れ図である。

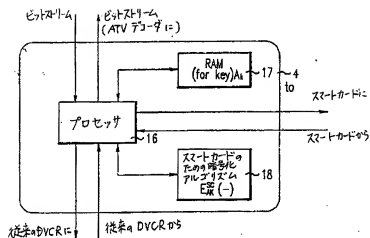
【符号の説明】

- 1、104 復調及び誤り訂正部
- 2、6 ATVデコーダ
- 3 スマートカード
- 4、8 複写防止処理部
- 11、16 プロセッサ

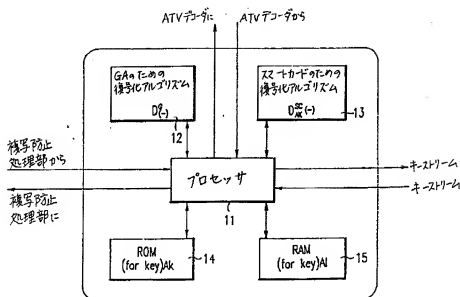
【図2】



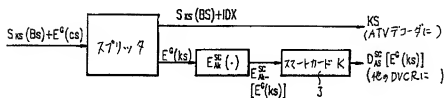
【図 8】



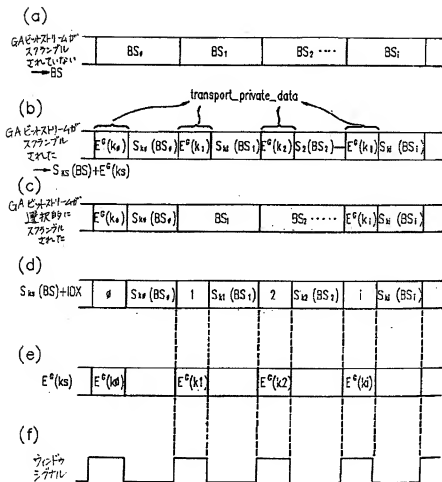
【図 9】



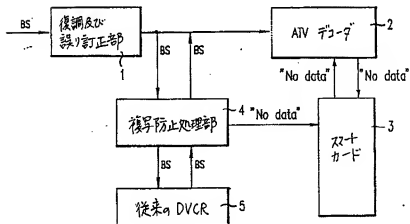
【図 10】



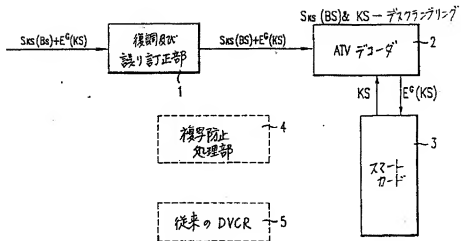
【図 11】



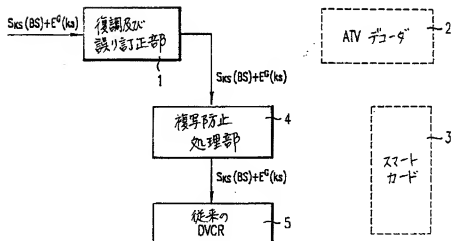
【図 12】



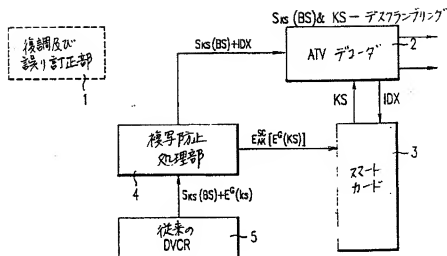
【図13】



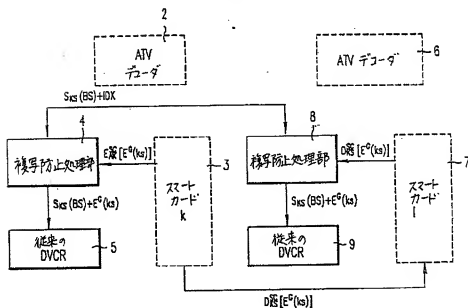
【図14】



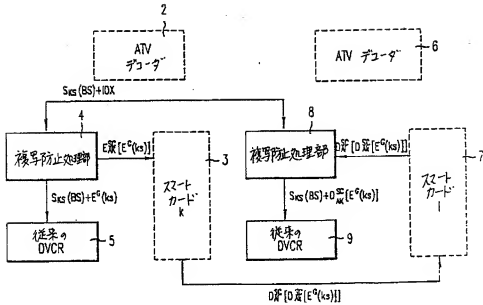
【図 15】



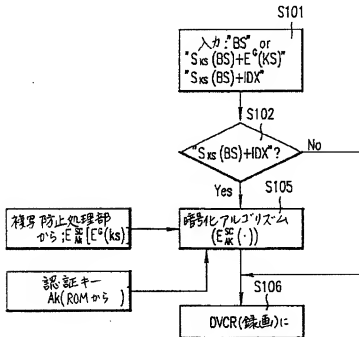
【図 16】



【図 17】

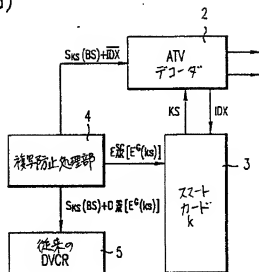


【図 19】

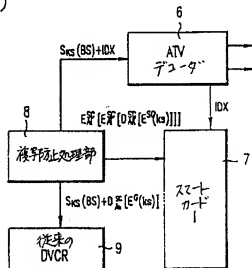


【図 18】

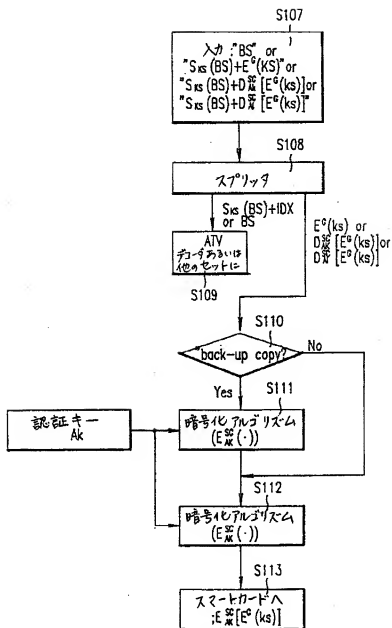
(a)



(b)



【図 20】



```

graph TD
    S114[ADPデータから:  
E*(KS) or IDX] --> S115{IDX}
    S115 -- Yes --> S118[符号化アルゴリズム  
(D*(.)) ]
    S115 -- No --> S116[符号化アルゴリズム  
(D*(.)) ]
    S118 --> S119{再符号化?}
    S119 -- Yes --> S116
    S119 -- No --> S120{back-up copy?}
    S120 -- Yes --> S121[符号化アルゴリズム  
(D*(.)) ]
    S120 -- No --> S116
    S121 --> S122[符号化アルゴリズム  
(D*(.)) ]
    S122 --> S123[スタートカードに:  
(ks) or Dn[Dn(E*(ks)) ]
    S123 --> S124[防止処理部に]
    S116 --> S117[ADPデータ:  
KS]
    S117 --> S124

```

【図 22】

